LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Yrityksen tietoturvan ulkoinen tarkastus

Robin Lindroos

Laurea-ammattikorkeakoulu

Yrityksen tietoturvan ulkoinen tarkastus

Robin Lindroos
Tietojenkäsittelyn tutkinto
Opinnäytetyö
Toukokuu, 20182018

Laurea-ammattikorkeakoulu **Tiivistelmä**
Tietojenkäsittelyn tutkinto
Tradenomi (AMK)

Robin Lindroos

Yrityksen tietoturvan ulkoinen tarkastus

Vuosi 2018 Sivumäärä 62

Tämän opinnäytetyön tavoitteena oli selvittää yrityksen tietoturvan nykytila. Opinnäytetyön tarkoitus oli auttaa yritystä täydentämään EU:n tietosuoja-asetukseen (GDPR) valmistautuessa puuttunutta dokumentaatiota laatimalla yleiskuvaus yrityksen tietoliikenne-, tietojärjestelmä-, tietoaineisto- ja käyttöturvallisuudesta sekä paikkaamaan havaitut puutteet.

Opinnäytetyön tietoperusta koostuu laadullisesta tutkimusmenetelmästä, tapaustutkimuksesta, KATAKRI-auditointikriteeristöstä, riskianalyysistä sekä erilaisten hyökkäys- ja puolustusmenetelmien kirjallisuudesta.

Tutkimuksen aikana ilmenneet havainnot kirjattiin yrityksen riskienhallintatyökaluun ja muistiinpanojen pohjalta laadittiin lopulliset tutkimustulokset. Havaitut puutteet laitettiin tärkeysjärjestykseen riskianalyysin tulosten perusteella, joka yhdisti riskin todennäköisyyden ja sen seurauksen vakavuuden.

Yrityksen tietoturva oli pääosin hyvällä tasolla eikä sen tietoverkkoihin, tietojärjestelmiin, aineistoihin tai henkilöstöön kohdistu välitöntä ulkoista tai sisäistä uhkaa. Vakavimpia puutteita oli salausratkaisuissa, järjestelmän kovennuksessa, turvallisuuteen liittyvien tapahtumien jäljitettävyydessä ja toimijoiden tunnistamisessa.

Toimeksiantajan antama palaute oli positiivista. Lopullista tuotosta arvioitiin tulosten analyyttisyydellä ja laadulla. Katakri-auditointityökalu sopi tutkimukseen hyvin ja tuloksia saatiin paljon aikaiseksi, joskin sellaisenaan se on tarkoitettu yrityksille, joilla on enemmän salassa pidettävää tietoa, joten harkintaa oli käytettävä jonkin verran sen sovittamiseksi kohdeyrityksen tarpeisiin.

Asiasanat: Katakri, tietoturva, auditointi, riskienhallinta, tietosuoja

Laurea University of Applied Sciences **Abstract**
Degree Programme in Business Information Technology
Bachelor's Thesis

Robin Lindroos

External audit of a company's information security

Year 2018 Pages 62

The objective of this thesis was to clarify the current state of a company's information security. The purpose of the thesis was to help the company to supplement their documentation, which was missing when they were preparing for the EU General Data Protection Regulation (GDPR) by composing a general overview of communications, system, data and operations security and to fix the detected shortcomings.

The knowledge base of this thesis consists of qualitative research method, case study, National Security Auditing criteria (KATAKRI), risk analysis and literature of various attack types and countermeasures.

The observations made during the investigation were recorded to company's risk management tool and the final research results were concluded from these notes. Detected vulnerabilities were prioritized based on the results of a risk analysis, which combined the probability and severity of the risk.

The information security of the company was generally on a good level and no immediate internal or external threats are posed to its networks, information systems, data or personnel. Cryptography, system hardening, traceability of security events and user identification had the most severe shortcomings.

Feedback given by the client was positive. The final product was evaluated based on its analytics and the quality of the results. Katakri-auditing tool was well suited for this research and a lot of results were achieved, although as such it's intended for organizations with more confidential data, so a bit of judgement had to be used for adapting it to client's needs.

Keywords: Katakri, information security, audit, risk management, data protection

Sisällys

1 Johdanto

Turvallisuudella on kaksi puolta. Pyrimme suojelemaan meille tärkeitä asioita, toisella puolella joku taas yrittää varastaa ne meiltä. Yrityksille tärkeää on heidän liiketoimintansa ja siksi he voivat joutua hyökkäyksen kohteeksi monestakin syystä. Taloudellinen hyöty, suosio tai vanha kauna ovat vain jäävuoren huippu. Teknologian kehityksen myötä tietoa on enemmän kuin ennen ja hyökkääjille on avautunut uusia ovia, sillä turvallisuus seuraa vasta askeleen perässä. Sekään ei enää riitä, että hyökkääjät pidetään ulkona, vaan yritys voi epähuomiossa tuhota tiedon itse.

Opinnäytetyön toimeksiantaja oli kylmäalanyritys, jossa työskentelee noin 300 työntekijää. Ennen opinnäytetyötä kohdeyrityksellä ei ollut selkeää kokonaiskuvaa tietoturvan nykytilasta ja vaikka muutokset kirjataan ulkoisen palveluntoimittajan tikettijärjestelmään, niin dokumentaatio rajoittui lähinnä verkkokuvaan, jossa on määritelty tietoliikenneyhteydet eri palveluiden välillä. Yritys päätyi ulkoistamaan tehtävän, koska se tarjosi uskottavamman analyysin tilanteesta, kuin yrityksen sisäisen työntekijä teettämä tutkimus.

Valitsin tämän aiheen opinnäytetyölle, sillä siinä oli kyse oikeasta työelämän tilanteesta. Koin tutkimusprojektin olevan looginen jatkumo jo suoritetuille opinnoilleni ja tutkimus hyödytti selkeästi molempia tutkimuksen osapuolia. Arvelin myös pystyväni hyödyntämään tutkimuksesta saavutettuja kokemuksia tulevaisuudessa.

Tutkimuksessa ja aineiston keräämisessä hyödynnettiin laadullista tutkimusmenetelmää, sen tutkimustyyppiä tapaustutkimusta, auditointia ja riskianalyysiä. Alustava tutkimusongelma oli ”miten saada yrityksen tietoturvan nykytila selville?”. Tutkimusaineisto kerättiin pääosin teemahaastatteluilla.

Aihealue päätettiin rajata pelkästään Katakrin tekniseen osioon, jotta työmäärä pysyisi kohtuullisessa mittakaavassa. Tämä sopi sekä toimeksiantajalle että opinnäytetyön tekijälle, sillä kaikista Katakrin osa-alueista tekninen oli EU:n yleisen tietosuoja-asetuksen voimaan astumista ajatellen kaikkein tärkein. Toimeksiantajalla oli myös teknisestä osa-alueesta kaikkein vähiten tietoa ja se oli tutkijan mielestä myös kaikkein kiinnostavin.

1.1 Tutkimuksen tavoite

Yrityksen ongelmana oli, ettei heillä ollut tarkkaa tietoa verkon aktiivilaitteiden, järjestelmien tai tietoaineistojen tietoturvasta, jotka ovat ulkoisen palveluntoimittajan vastuulla. Tästä syystä ei ollut dokumenttejakaan, mistä aiheutui huomattavasti vaivaa yrityksen valmistautuessa EU:n yleiseen tietosuoja-asetukseen, jota alettiin soveltaa toukokuussa. Ainoastaan muutokset kirjataan nykyään palveluntoimittajan tikettijärjestelmään.

Opinnäytetyön tavoitteena oli saada selville yrityksen teknisen tietoturvan nykytila, dokumentoida havainnot ja laatia korjaustoimenpiteitä havaituille puutteille. Yrityksen toivomuksena oli myös, että se voisi laatia tietotilinpäätöksen opinnäytetyön perusteella. Tietotilinpäätös on vapaaehtoinen asiakirja, jolla yritys voi täydentää lain pakottamia hallinnollisia raportteja, kuten tilinpäätöksiä ja toimintakertomuksia tai hyödyntää esimerkiksi tietosuojalain muuttuessa (Laadi tietotilinpäätös 2012).

2 Teoreettinen viitekehys

Tässä luvussa kuvaillaan yleisesti tämän opinnäytetyön kannalta kannalta tärkeät käsitteet auditointi, KATAKRI, riskianalyysi ja EU:n yleinen tietosuoja-asetus. Teoreettisen viitekehyksen jälkeen kuvaillaan opinnäytetyössä käytettyjä tutkimusmenetelmiä. Tutkimusmenetelmien jälkeen siirrytään opinnäytetyön toteutukselliseen osioon.

2.1 Auditointi

Auditointi on paikan päällä suoritettavaa toimintaa, kuten tarkastus tai tutkimus, jolla vahvistetaan, että prosessi tai järjestelmä on määräysten tai vaatimusten mukainen. Auditointiprosessi on systemaattinen, itsenäinen ja dokumentoitu. Auditointiprosessilla saavutetaan tietoja, jotka ovat tarkastuksen kannalta oleellisia ja tarvittaessa varmistettavissa. Tietoja arvioidaan objektiivisesti, jotta voidaan päätellä, miten auditoinnille määritelty kriteeristö, menettelytapa tai vaatimustaso täyttyy. (What is auditing? 2018.)

Turvallisuusauditointi on vuorovaikutteista. Alussa tutustutaan kohdeorganisaation turvallisuusdokumentaatioon, jonka jälkeen auditoija käy tarkistettavat kohteet läpi muun auditointiryhmän kanssa etukäteen tehdyn suunnitelman pohjalta. Vakavista puutteista ilmoitetaan välittömästi, jotta korjaustoimenpiteet saadaan nopeasti työn alle. (KATAKRI – Kansallinen turvallisuusauditointikriteeristö, 2011).

Auditoinnin voi toteuttaa organisaation sisäisen työntekijä (ensimmäinen osapuoli), asiakas/toimittaja (toinen osapuoli) tai kokonaan ulkoinen toimija (kolmas osapuoli). Auditointiprosessi koostuu pääosin valmistautumisesta, tietojen keräämisestä eli kenttätyöstä, raportoinnista ja jatkotoimenpiteistä/lopetuksesta (What is auditing? 2018). Auditointia varten voidaan kerätä tietoja havainnoinnilla, tutkimalla yrityksen dokumentteja ja erilaisilla haastatteluilla (Cochran, 2016; IS Audit and Assurance Guideline 2205 Evidence 2014).

Tietojen analysoinnissa olisi hyvä ottaa huomioon seuraavat kaksi asiaa: Ensinnäkin tiedot ovat riittävän asianmukaisia, kunhan ne tarjoavat kohtalaisen hyvän perustan tutkimustuloksen tai johtopäätöksen tukemiseksi. Toiseksi, tiedot ovat lähtökohtaisesti

luotettavampia, kun ne ovat suullisen sijaan kirjallisessa muodossa ja/tai tulevat suoraan asiantuntijoilta. (IS Audit and Assurance Guideline 2205 Evidence 2014.)

2.2 Katakri-auditointityökalu

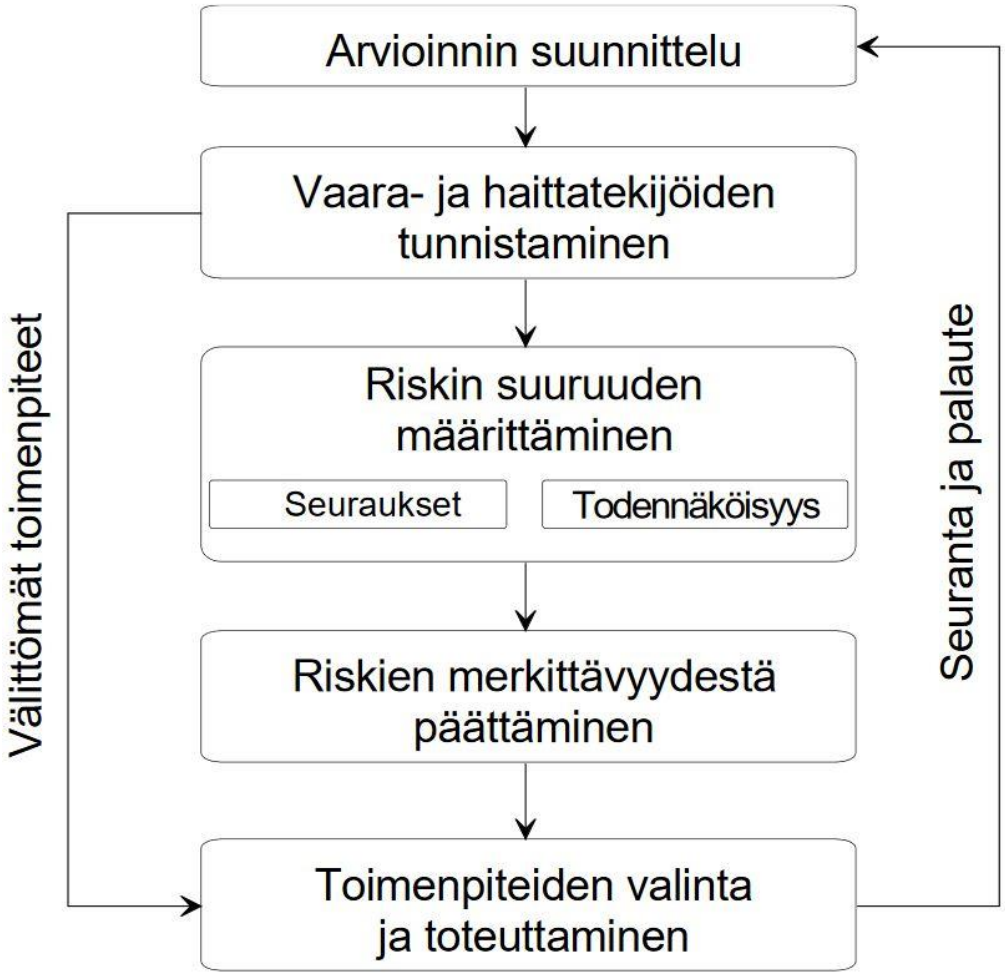
Katakri-auditointikriteeristö on viranomaisille suunnattu työkalu, jolla voidaan arvioida organisaation kykyä suojata viranomaisen salassa pidettävää tietoa. Siihen on koottu vähimmäisvaatimukset Suomea sitovista lainsäädännöistä ja kansainvälisistä sopimuksista. Sitä voidaan käyttää myös muiden yritysten turvallisuustyön kehittämiseen. Katakrin vaatimukset on jaettu turvallisuusjohtamiseen, fyysiseen turvallisuuteen ja tekniseen turvallisuuteen. (Katakri - Tietoturvallisuuden auditointityökalu viranomaisille 2015.)

Katakrin turvallisuusjohtamisosion vaatimuksilla pyritään varmistamaan, että yrityksellä on riittävät hallinnollisen turvan ja henkilöstöturvan turvatoimet paikallaan, toimiva turvallisuudenhallintajärjestelmä sekä asianmukaisesti toimiva henkilöstö. Fyysisen turvallisuuden vaatimusten lähtökohtana on, etteivät salassa pidettävät tiedot paljastu henkilöille, joilla ei ole niihin oikeuksia. Fyysisillä turvatoimilla estetään tunkeutumiset, havaitaan ja ehkäistään luvattomia toimia sekä rajataan henkilöstön luokitus ja käyttöoikeudet tiedonsaantitarpeen mukaan. (Katakri - Tietoturvallisuuden auditointityökalu viranomaisille 2015.)

Teknisen tietoturvallisuuden osa-alueen vaatimukset keskittyvät varmistamaan riittävät turvallisuusjärjestelyt organisaation sähköisissä käyttöympäristöissä. Tekninen tietoturvallisuus on jaettu tietoliikenne-, tietojärjestelmä-, tietoaineisto- ja käyttöturvallisuuteen. Osa-alueen vaatimukset sellaisenaan edellyttävät tulkintaa kohdeympäristön riskienarvioinnin perusteella, mutta osioiden lisätietokenttiin on listattu myös toteutusesimerkkejä, joilla vähimmäisvaatimukset voidaan täyttää useimmissa ympäristöissä. (Katakri - Tietoturvallisuuden auditointityökalu viranomaisille 2015.)

2.3 Riskianalyysi

Riskianalyysillä tarkoitetaan järjestelmällisiä toimenpiteitä, joilla pyritään tunnistamaan tietoturvallisuuden uhkia ja haavoittuvuuksia sekä arvioimaan toteutuvien uhkien seurauksia. Riskianalyysillä pyritään vastaamaan kysymyksiin kuten: ”Mitä voi sattua?”, ”Mitä siitä voi seurata?”, ”Miten suuri on aiheutuva riski?” ja ”Mitkä ovat suurimmat riskit?”. Tulosten raportointi ja perustelut sisältyvät myös riskianalyysiin. (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003.)



Kuvio 1: Riskien arvioinnin ja hallinnan vaiheet (Riskien arviointi työpaikalla –työkirja, 2015.)

Riskianalyysin ensimmäinen tehtävä on uhkien tunnistaminen. Tunnistamisen jälkeen niiden todennäköisyys ja seurausten vakavuus arvioidaan. Yrityksellä on useita vaihtoehtoja havaittujen riskien hallintaan (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003.):

1. Riski voidaan välttää pidättäytymällä kyseisestä toiminnasta.
2. Riski voidaan poistaa, mikä voi tosin aiheutua uusia riskejä.
3. Riski voidaan siirtää esimerkiksi vakuutuksella tai sopimuksella jollekin toiselle.
4. Riskin todennäköisyyttä tai vakavuutta voidaan rajata erilaisilla kontrolleilla.
5. Yritys voi pitää riskin omalla vastuullaan, eli otetaan tietoinen riski siitä, että uhka voi toteutua.

Riskejä voidaan pienentää teknisillä, organisaatiollisilla tai yksilöllisillä toimenpiteillä. Teknisiä toimenpiteitä ovat laite- ja tilaratkaisut, konesuojaukset, hälytinjärjestelmät, tekniset varmennukset sekä huollon ja kunnossapidon parannukset. Organisaatiollisia toimenpiteitä ovat yhteiset toimintaohjeet, valvonnan ja seurannan parantaminen, tiedonkulun ja työnsuunnittelun kehittäminen sekä vastuusta sopiminen. Yksilöllisiä toimenpiteitä ovat työvälineiden hankinta, ohjeistus, perehdyttäminen, koulutus sekä työaika- ja työparijärjestelyt. (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003.)

Kaikkia riskejä ei tarvitse eikä välttämättä kannatakaan poistaa. Jatkotoimenpiteissä on syytä edetä suurimmista riskeistä pienempiin miettien samalla, kuinka paljon yritys on valmiina panostamaan niihin. Usein mahdollisia uhkia löytyy niin paljon, että kaikkia on mahdoton hoitaa, joten tärkeintä on keskittyä isoimpiin riskeihin, jotka vaativat ratkaisua kiireellisimmin. (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003.)

2.4 EU:n yleinen tietosuoja-asetus

Suomen ja Euroopan unionin tietosuojalait uudistuvat ja uutta EU:n yleistä tietosuoja-asetusta aletaan soveltaa 25.5.2018 alkaen kaikissa EU:n jäsenmaissa. Uusi tietosuojalaki asettaa uusia velvoitteita siitä, miten henkilötietoja tulee käsitellä. Henkilötietojen kerääminen, tallettaminen, järjestäminen, käyttö, siirtäminen, muuttaminen, yhdistäminen, suojaaminen, poistaminen, tuhoaminen ja muut vastaavat toimenpiteet lasketaan henkilötietojen käsittelemiseksi. (Tietosuoja-aiheista sanastoa 2013). Henkilötietojen käsittelyä koskevien velvoitteiden laiminlyönnistä voi seurata sanktioita, kuten henkilötietojen käsittelykielto tai sakkoja. (EU:n tietosuojauudistus 2018).

3 Tutkimusmenetelmät

Opinnäytetyön tutkimuskysymykseksi muodostui: ”Miten saada yrityksen tietoturvan nykytilanne selville?”, koska tieto oli niin hajanaista ja monessa eri paikassa. Alakysymyksiä olivat ”Miten verkon aktiivilaitteet ja järjestelmät konfiguroidaan turvallisiksi?”, ”Miten tietoaineistot suojataan?”, ”Miten käyttäjiä on ohjeistettu tietoturvan suhteen?”, ”Miten EU:n tietosuoja-asetus vaikuttaa yrityksen tietojenkäsittelyyn?” ja ”Millaisia puutteita tietoturvassa on?”. Lisäksi piti vielä selvittää: miten havaitut puutteet korjataan?

3.1 Laadullinen tutkimus

Tosielämän tilanteiden kokonaisvaltainen kuvaaminen on Hirsjärven, Remeksen ja Sajavaaran (2009, 161) mukaan laadullisen tutkimuksen lähtökohta. Tutkimuksella pyritään Kanasen (2013, 26) mukaan ymmärtämään tiettyä ilmiötä ja selittämään sen koostumusta, tekijöitä ja tekijöiden välisiä suhteita. Kananen (2013, 26) jatkaa, ettei laadullisessa tutkimuksessa voida

esittää tarkkoja kysymyksiä, sillä ilmiö on tuntematon, vaan tiedot on hankittava tutkittavien tekijöiden kautta.

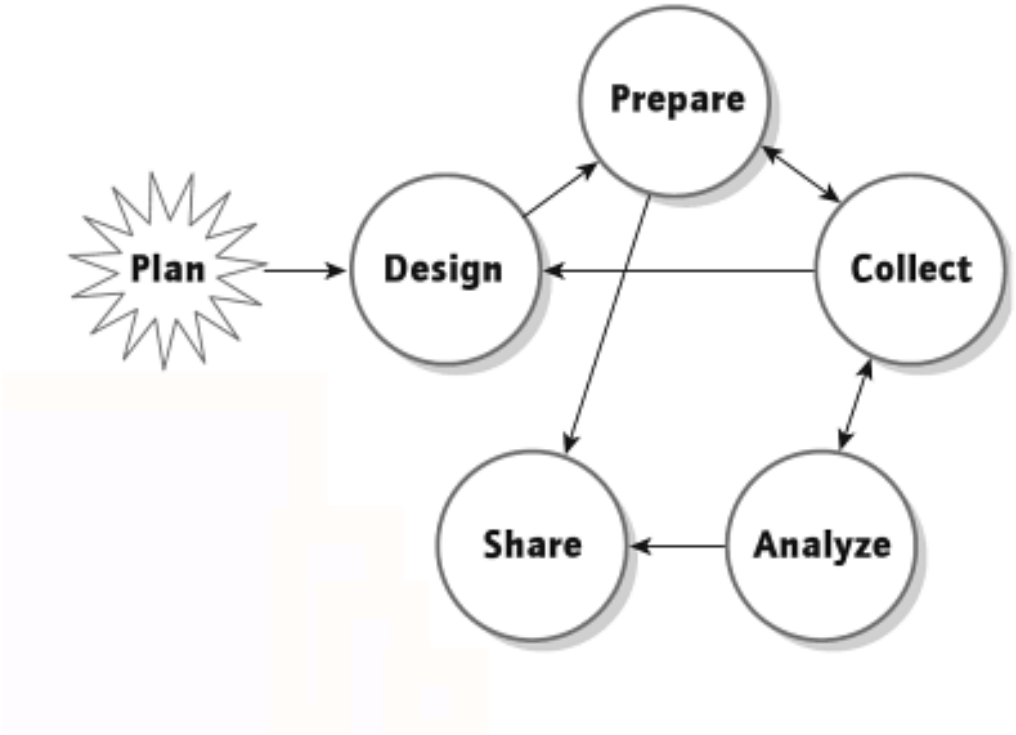
Laadullisen tutkimuksen tyypillisiä piirteitä ovat tutkimusaineiston koonti sen todellisessa ja luonnollisessa tilanteessa, ihmisten käyttö tiedonkeruussa sekä teema- ja ryhmähaastatteluiden, havainnoinnin ja dokumenttien suosiminen aineiston keruussa. Tulosten analysointi on induktiivista, eli lähtee liikkeelle käytännöllisistä ilmiöistä, mutta päätyy teoreettisiin. (Hirsjärvi ym. 2009, 164; Kananen 2013, 23 - 27).

Laadullisesta tutkimuksesta käytetään myös nimitystä aineistolähtöinen tutkimus, koska siinä aineisto ohjaa tutkimusta. Tutkimus ei etene tiukasti vaihe vaiheelta, sillä joskus joudutaan palaamaan aiempaan tutkimusprosessin vaiheeseen, esimerkiksi uuden havainnon takia tai mikäli huomataan, että tieto on riittämätöntä. Tietoa analysoidaan jatkuvasti samalla kun sitä kerätään eikä vasta sen jälkeen, kun ne on jo kerätty. (Kananen 2013, 90.)

3.2 Tapaustutkimus

Tapaustutkimus on laadullisen tutkimuksen tutkimisstrategia, jolla on tarkoitus perehtyä tämänhetkisiin ilmiöihin hyvin syvällisesti ja kuvata ne mahdollisimman kattavasti. Se pyrkii vastaamaan tutkimuskysymyksiin, miten, kuinka ja miksi? Tapaustutkimus teetetään tutkittavan ilmiön kannalta luonnollisessa ympäristössä eli oikeassa kontekstissa. (Hirsjärvi ym. 2009, 134-135; Kananen 2013, 54; Yin 2009, 10 - 11).

Yin (2009, 10-11) määrittelee, että tapaustutkimus on ensisijainen tutkimusmenetelmä tutkiessa tämänhetkisiä tapahtumia, silloin kun muuttujiin ei voida vaikuttaa. Yin (2009, 24 – 25) jakaa tapaustutkimustyön viiteen osaan: tutkimuksen suunnitteluun, tiedonkeruun valmisteluun, tietojen keräämiseen, tietojen analysointiin ja raportointiin. Tutkimuksen suunnittelun aikana tulee määritellä tutkimuskysymykset, analysoinnin kohteet ja kriteeristö, jolla havainnoista vedetään johtopäätökset (Yin 2009, 26 – 30).



Kuvio 2: Tapaustutkimusprosessi. Lineaarinen, mutta iteratiivinen (Yin 2009, 1 – 2.)

Tutkijan olisi hyvä valmistautua tapaustutkimukseen hiomalla sen kannalta tärkeitä taitoja, kuten haastattelu- ja kuuntelutaitoa, mukautumista, joustavuutta, ennakkoluulottomuutta ja puolueettomuutta (Yin 2009, 69 – 72). Tapaustutkimuksen tietoaineistot jaotellaan dokumentaatioon, teemahaastatteluihin, suoraan havainnointiin ja osallistuvaan havainnointiin. (Hirsjärvi ym. 2009, 135; Kananen 2013, 78; Yin 2009, 101 – 102.)

Dokumentaatioksi lasketaan kirjeet, muistiot, sähköpostit, päiväkirjat, kalenterit, uutisleikkeet, esityslistat, pöytäkirjat, muut kirjalliset tapahtumaraportit, organisaation hallinnolliset dokumentit ja tutkielmat. Dokumenttien vahvuuksia tiedonkeruun kannalta ovat niiden muuttumattomuus, pysyvyys, yksityiskohtaisuus, tietojen tarkkuus ja kattavuus. Tapaustutkimuksen kannalta dokumenttien tärkein tehtävä on tukea muista lähteistä saatuja väitteitä. Dokumenttien huono puoli on se, että ne voivat olla hankalasti saatavilla ja sisältää puolueellista tietoa tai kirjoittajan tekemiä virheitä. (Kananen 2013, 80; Yin 2009, 101-103).

Teemahaastattelulla voidaan kohdentaa kysymykset tutkittavaan ilmiöön paremmin kuin dokumenteilla. Haastattelija voi kysyä sekä faktoista, että vastaajan mielipiteistä. Teemahaastattelun kysymykset ja vastaukset pohjautuvat aitoon tilanteeseen. Teemahaastattelun uhkana ovat heikot kysymykset ja vastaukset, puolueellisuus ja liika

myötäily. Haastateltava voi antaa vastauksia, joita halutaan kuulla. (Kananen 2013, 80 – 81; Yin 106 – 107.)

Havainnointi voi olla suoraa tai osallistuvaa. Osallistuvassa havainnoinnissa tutkija osallistuu itse tutkittavan kohteen tapahtumiin, mikä tarjoaa paremman näkemyksen tutkimukseen osallistuvien ihmisten näkökulmasta. Havainnoinnin etuna on, että se perustuu aitoon tilanteeseen ja sitä pidetään yhtenä tehokkaimmista tiedonkeruumenetelmistä, mutta se voi olla aikaa vievää ja tutkijalla on todella suuri vaikutus sen onnistumiseen, mikä vielä korostuu osallistuvassa havainnoinnissa. Tutkija saattaa tahattomasti vaikuttaa tapahtumiin eivätkä tutkimukseen osallistuvat henkilöt eivät välttämättä toimi tutkimusolosuhteissa samalla tavalla kuin tavallisesti. (Kananen 2013, 81; Yin 2009, 109 – 113.)

Tapaustutkimuksen tietoja analysoidessa on hyvä aloittaa ensin pienellä kysymyksellä ja tunnistaa sitten tieto, joka vastaa kysymykseen. Kyseisestä tiedosta vedetään alustava johtopäätös miettien samalla, kuinka tiedon voisi esitellä muille, jonka jälkeen siirrytään isompaan kysymykseen, kunnes tiedolla voidaan vastata päätutkimuskysymykseen. (Yin 2009, 128.)

Tapaustutkimuksella on useita aineiston tulkintamenetelmiä, joilla pyritään löytämään selityksiä kohdeilmiöille (Kananen 2013, 110; Yin 2009, 136 – 150). Selityksen rakentaminen on yleisin aineistontulkintamuoto perinteisissä tapaustutkimuksissa (Kananen 2013, 112). Siinä ilmiöille pyritään laatimaan syvällinen ja kattava kuvaus tai kirjoitetaan se tarinan muotoon (Kananen 2013, 112; Yin 141).

Tapaustutkimusta raportoidessa on syytä ottaa huomioon kohderyhmä, kenelle kirjoitetaan. Mikäli kohderyhmää ei ole määritelty tai kohderyhmän tarpeita ei huomioida, kirjoittaja sortuu herkästi itsekeskeiseen kirjoitustyyliin (Yin 2009, 170). Esimerkillisessä tapaustutkimuksessa kirjoittaja kykenee esittämään sen verran paljon tietoa, että lukija pystyy tekemään omat johtopäätökset sen perusteella (Yin 2009, 188-189).

4 Auditointiprosessi ja tulokset

Opinnäytetyö oli tutkimustyypiltään laadullinen tutkimus. Opinnäytetyön tavoitteena oli hahmottaa ja selvittää millä tasolla yrityksen tietoturva on ja mallintaa mahdollisimman kattava dokumentaatio siitä. Näin ollen tutkimus keskittyy ilmiöön, joka on jo olemassa, mutta tarkka lopputulos on hämärän peitossa ja täytyy selvittää muilla keinoilla. Opinnäytetyössä tehdään tutkimustyötä ihmisten ja kohdeilmiön kanssa samassa tilassa ja aidoissa olosuhteissa, jotka myös puoltavat laadullista tutkimusmenetelmää.

Tapaustutkimus sopi tutkimusmenetelmäksi opinnäytetyöhön, sillä tutkimuskysymyksissä oli huomattavan paljon ”miten?” kysymyksiä, tapahtumien käyttäytymiseen ei tarvinnut eikä saanut puuttua ja tutkimuksen kohteena oli tämänhetkinen ilmiö. Tutkimuksen aineisto tultiin

keräämään olemassa olevaa dokumentaatiota tutkimalla ja teemahaastatteluilla. Tutkittavasta ilmiöstä myös pyrittiin kuvailemaan kaikki mahdollisimman kokonaisvaltaisesti.

Nykytilanne päätettiin selvittää auditoinnilla, koska tarkoituksena oli hankkia tutkimuksen kannalta oleellisia tietoja sekä varmistaa, että tietoturva täyttää sille asetetut määritelmät. Tässä opinnäytetyössä auditointi oli ulkoista, sillä tarkastaja eli opinnäytetyön tekijä ei ollut tekemisissä yrityksen kanssa ennen opinnäytetyötä. Auditoinnilla on myös huomattavan paljon yhteisiä piirteitä sekä laadullisen tutkimuksen että tapaustutkimuksen kanssa, kuten aineistonkeruumenetelmät ja aidot olosuhteet.

Tutkimuksessa toteutetun auditoinnin vaatimuskriteereinä päätettiin käyttää KATAKRI-auditointityökalun vaatimuksia, koska ne tarjosivat tutkimuskysymysten kannalta oleellisen, kattavan sekä kohtalaisen helppolukuisen listan tarvittavista vaatimuksista yrityksen tietoturvan arviointia ja kehittämistä varten. Auditoinnin mittakaava rajoittui työmäärän ja tutkimuskysymyksen vuoksi pelkästään Katakrin tekniseen osioon, koska se oli myös EU:n tietosuoja-asetuksen (GDPR) soveltamisajankohdan vuoksi selkeästi tärkein osio, sillä kyseinen osio sisältää muun muassa tietoaineisto- ja käyttöturvallisuuden, joissa käsitellään salassa pidettävän tiedon suojaamista. Tavoitteena ei ollut, että tarkastuksen jälkeen yritys läpäisisi kaikki Katakrin vaatimukset, sillä sellaisenaan se on suunnattu arvioimaan yrityksen kykyä suojella erittäin salaista tietoa, vaan selvittää millä tasolla tietoturva on yleisesti ja löytää kultainen keskitie työntekijöiden vaatimusten, kustannusten ja turvallisuuden välillä (Katakri - Tietoturvallisuuden auditointityökalu viranomaisille 2015).

Katakrin toisen ja kolmannen version välillä mietittiin pitkään, sillä vaikka kolmas versio on uudempi, niin toisella versiolla on yksi merkittävä etu kolmanteen verrattuna: Toisessa versiossa on viranomaisvaatimuksista erillinen ”Elinkeinoelämän suositukset” vaatimustaso, joka on tarkoitettu pienempien yritysten turvallisuuden kehitystyöhön, silloin kun ei ole tarpeen käsitellä salassa pidettäviä tietoja. Kolmannen version vaatimukset jättävät myös tarkastajalle huomattavasti enemmän tulkinnan varaa, kuin toisen version vaatimukset jotka ovat joustamattomia, joten toinen versio on yksinkertaisempi, varsinkin aloittelevalle tarkastajalle.

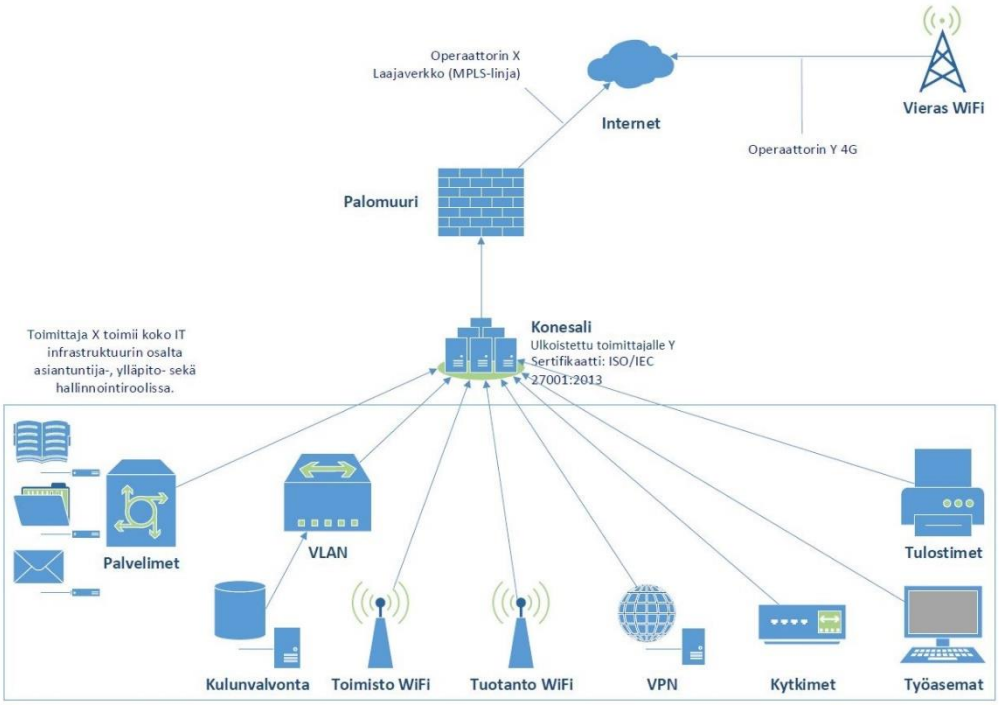
Lopulta Katakrin kolmanteen versioon päädyttiin paristakin syystä:

1. Monimutkaisuudesta johtuen sen osaaminen tarjoaa todennäköisesti paremmat eväät jatkossa myös muiden auditointikriteeristöjen käyttöön.

2. Kolmannen version toteutusesimerkit ajavat useimmissa tapauksissa saman asian, kuin aiemmat elinkeinoelämän suositukset.

3. Toimeksiantajalla oli GDPR tietosuoja-asetusta varten ulkopuoliselta konsultointiyhtiöltä hankittu riskienhallinta- ja dokumentointipalvelu, josta löytyi valmiina Katakrin kolmosversion vaatimukset. Työkalun ansiosta muistiinpanojen ja havaintojen dokumentointi oli todella helppoa.

Tutkimuksen aikana opinnäytetyöntekijä tapasi säännöllisesti IT-päällikön, palveluntoimittajan ja asiantuntijan kanssa palavereissa. Dokumentaatiota oli odotettua vähemmän ja se rajoittui lähinnä yksinkertaiseen verkkokuvaan, jossa oli kuvattu tietoliikenneyhteydet eri laitteiden välillä. Tutkijalla ei myöskään ollut pääsyä palveluntoimittajan tikettijärjestelmään.

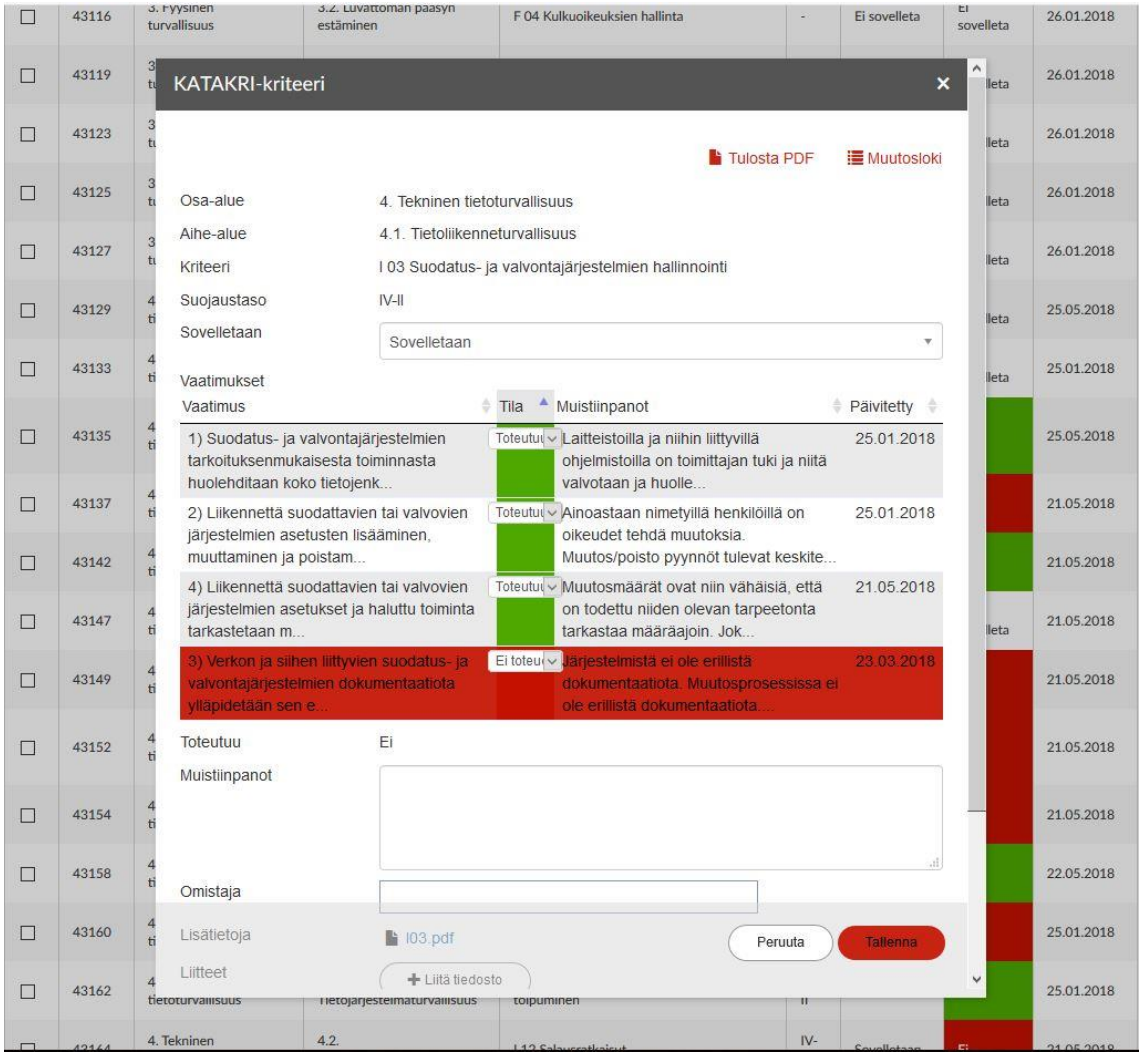


Kuvio 3: Yrityksen verkko ja sen toimittajat (Asiantuntija X 2018.)

Tutkija toimi palavereiden puheenjohtajana ja esitteli aluksi auditoinnin tarkoituksen, vaatimukset ja tavoitteen. Palavereiden aikana tutkija kysyi Katakrin vaatimuksiin liittyviä kysymyksiä ja kirjasi vastauksia yrityksen riskienhallintatyökaluun. Haastattelukysymyksiä ei suunniteltu etukäteen, sillä Katakrin kolmas versio jätti tutkijalle niin paljon tulkinnanvaraa, että strukturoitua haastattelua oli hankala suunnitella vaatimusten pohjalta, joten keskustelu oli hyvin avointa.

Tarkastus eteni lineaarisessa järjestyksessä ensimmäisestä vaatimuksesta viimeiseen. Tarkentavia kysymyksiä kyseltiin sitä mukaan, kun Katakrin vaatimukset lähtivät avautumaan. Kun tutkija koki, että tietoa oli kasassa tarpeeksi tapauksen kuvaamiseksi raporttiin,

siirryttiin eteenpäin. Jos jokin tarkastuksessa käsitelty kohta ei selvinnyt heti, tilanne selvitettiin ja palattiin myöhemmin asiaan sähköpostitse.

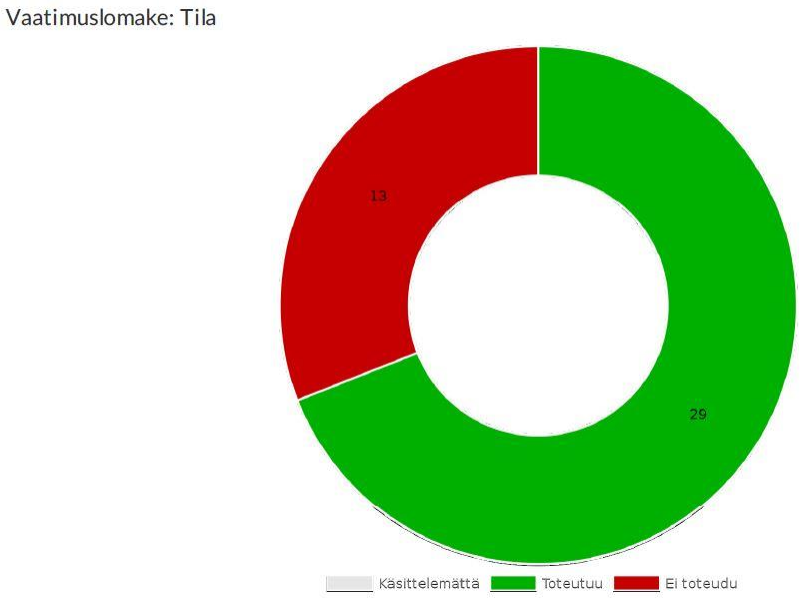


Kuvio 4: Ruutukaappaus Yrityksen riskienhallintatyökalusta

Tutkimuksen aikana joitakin Katakrin teknisen osion vaatimuksia ei sovellettu. Joko niiden riskien koettiin olevan olematon, niille ei nähty tarvetta tai sitten korjaustoimenpiteet olisivat aiheuttaneet suunnatonta vaivaa yrityksen työntekijöille siitä saavutettavaan hyötyyn nähden. Esimerkiksi hajasäteily jätettiin raportin ulkopuolelle, koska se koskee lähinnä vain erittäin salaisten tietojen suojaamista (Sähkömagneettisen hajasäteilyn aiheuttama tietoturvariskien ehkäisyn periaatteet 2013).

Kun kaikki Katakrin teknisen osa-alueen sovellettavat vaatimukset oli täytetty, tutkija laati nykytilanneanalyysin riskienhallintatyökaluun kirjattujen muistiinpanojen perusteella. Kaikkien osa-alueiden yhteensä 42:sta vaatimuksesta 29 täyttyi. Ei toteutuneiden vaatimusten määrä voi tuntua aluksi suurelta, mutta jokaisella kriteerillä voi olla useampi vaatimus ja

vaikka kaikkia kriteerin vaatimuksia ei noudatettaisikaan, niin ne oli laskettava riskienhallintatyökalussa mukaan, jos yhtäkin vaatimusta sovellettiin.

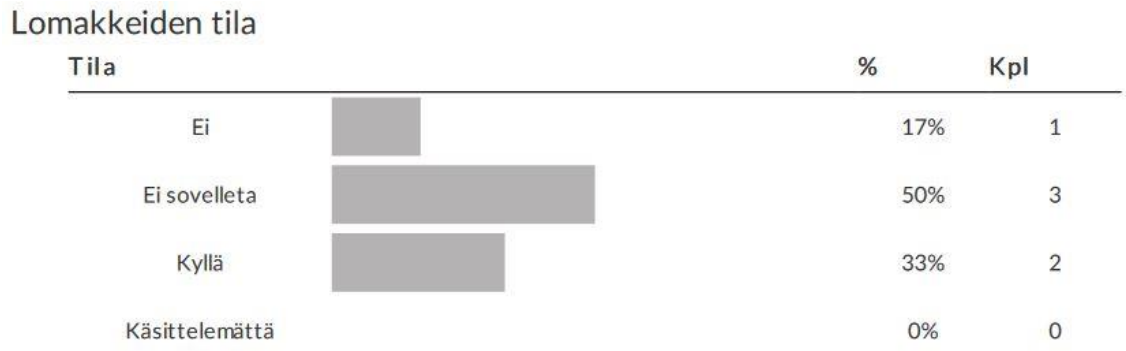


Kuvio 5: Kaikkien sovellettavien KATAKRI-kriteeristön vaatimusten tulokset (Yrityksen riskienhallintatyökalun raportti 2018.)

Nykytila-analyysi perustuu tutkimuksen aikana yrityksen riskienhallintatyökaluun kirjatuista tutkimustuloksista. Osion rakenne koostuu Katakri-auditointityökalun teknisen tietoturvan neljästä osa-alueesta. Seuraavissa alaluvuissa on kuvattu yrityksen tietoturvan nykytilanne.

4.1 Tietoliikenneturvallisuus

Katakrin Tietoliikenneturvallisuus osa-alue käsittelee yrityksen tietoverkon rakenteellisia ja liikennöllisiä turvallisuusvaatimuksia. Muutama kriteeri jouduttiin rajaamaan tutkimuksen ulkopuolelle, sillä joitakin ohjestuksia verkon rakenteellisista vaatimuksista ja vyöhykkeistämisestä oli hyvin hankala soveltaa järkevästi näin pieneen verkkoon. Langattomia verkkoja koskeva ohjeistus jätettiin myöhemmin soveltamatta, sillä riskit koettiin hyvin vähäisinä ja nykyinen suojaus riittävänä.



Kuvio 6: Tietoliikenneturvallisuuden tulokset (Yrityksen riskienhallintatyökalun raportti 2018.)

Julkinen verkko on erotettu yrityksen sisäisestä verkosta palomuurilla ja etäyhteyksissä VPN:llä. Langaton toimistoverkko ja tuotantoverkko on eroteltu toisistaan. Koko langaton verkko on myös suojattu WPA2-tekniikalla ja osa langattomista verkoista lisäksi myös Active Directory-ryhmällä WLAN-users. Päätelaitteet vahvistavat kohdeverkon sertifikaatilla, joka estää Man-in-the-Middle tyyppiset istuntokaappaukset. (Liite 1)

Yrityksen sisältä sen ulkopuolelle menevää liikennettä ei ole erikseen salattu, mutta palveluntarjoajalta on hankittu yrityksen konesalista pois päin kulkevalle liikenteelle oma (MPLS) yhteys, jonka läpi ei kulje muuta kuin yrityksen omaa dataa. Etäkäyttäjät käyttävät TLS-salattua VPN yhteyttä. Kaikki ulkopuolelta tuleva liikenne on oletuksena estetty ja sallittu vain tarvittava (default-deny). (Liite 1)

Laitteistoilla ja niihin liittyvillä ohjelmistoilla on toimittajan tuki ja niitä valvotaan ja huolletaan. Ainoastaan nimetyillä henkilöillä on oikeudet tehdä muutoksia niiden asetuksiin. Muutos/poisto pyynnöt tulevat keskitetysti IT-päälliköltä. Verkon valvonta- ja suodatusjärjestelmistä tai niiden muutoksista ei ole erillistä dokumentaatiota, mutta muutospyynnöt kirjataan toimittajan tikettijärjestelmään. (Liite 1)

Jokainen muutos tarkastetaan käyttöönottohetkellä, mutta niiden määrät ovat niin vähäisiä, että niiden määräaikaistarkastuksia ei tehdä. Kaikki palomuurisäädöt ja -konfiguraatiot varmuuskopioidaan ja niitä säilytetään asianmukaisesti. Hallintayhteydet on rajattu sisäverkkoon ja käyttöoikeudet annettu vain nimetyille henkilöille. Ulkopuoliset toimijat, jotka tarvitsevat hallintoyhteyksiä käyttävät VPN:ää ja heillä on käyttöoikeudet vain hallinnoimiinsa järjestelmiin. (Liite 1)

Langattomia verkkoja tulisi käsitellä kuin julkista verkkoa ja näin kannettavien työasemien käyttäminen langattomassa verkossa tulisi edellyttää VPN:n käyttöä (Katakri - Tietoturvallisuuden auditointityökalu viranomaisille 2015). Vaatimus päätettiin kuitenkin rajata tarkastelun ulkopuolelle, sillä sen koettiin haittaavan käyttäjien työntekoa liikaa ja

langattomien verkkojen kuuluvuutta on pyritty rajoittamaan rakennuksen ulkopuolelle sijoittamalla tukiasemat kauemmaksi ulkoseinistä. (Liite 1)

4.2 Tietojärjestelmäturvallisuus

Tietojärjestelmäturvallisuus osa-alue käsittelee muun muassa järjestelmien pääsyoikeuksien hallintaa, haittaohjelmasuojausta ja käyttäjätilien todentamista. Lähes kaikkia Katakrin vaatimuksia päätettiin soveltaa, sillä ainoastaan hajasäteilyä koskevat vaatimukset jätettiin huomioitta. Tässä osiossa yrityksellä todettiin olevan eniten petrattavaa.

Kuvio 7: Tietojärjestelmäturvallisuuden tulokset (Yrityksen riskienhallintatyökalun raportti 2018.)

Yrityksen järjestelmissä ja verkkolevyillä oleva tieto on suojattu käyttöoikeuksin. Jokainen muutos dokumentoidaan tikettijärjestelmään. Oikeuksien saanti edellyttää hyväksyntää asianmukaiselta vastuuhenkilöltä ja domain user-tason käyttäjien toimia voidaan seurata. Automaattiprosessien ja järjestelmänvalvojien tilannetta olisi syytä tarkastella enemmän, sillä heidän tekojen tunnistaminen ja todentaminen voi olla hankalaa. (Liite 1)

Yrityksellä ei ole käytössä pelkästään yksilöllisiä henkilökohtaisia käyttäjätunnuksia, vaan käytössä on myös yhteiskäyttötunnuksia. Tämä on perusteltua tuotantoympäristössä, mutta vaatisi selkeästi sovitut ja dokumentoidut salasanojen hallintakäytännöt yhteiskäyttöisille tunnuksille. Henkilökohtaisten tunnusten tunnistamisessa ja todennuksessa käytetään turvallista tekniikkaa. Esimerkiksi salasanan resetointi vaatii käyttäjän tunnistusta paikan päällä, mutta yhteiskäyttötunnusten kohdalla on haasteita. (Liite 1)

Salasanan syötön epäonnistuminen liian monta kertaa peräkkäin aiheuttaa tunnuksen lukittumisen Windowsissa ja Active Directorya käyttävissä järjestelmissä, mutta ei kaikissa erillistä tunnusta käyttävissä järjestelmissä. Käyttäjiä on ohjeistettu hyvästä turvallisuuskäytännöstä salasanan valinnassa ja käytössä. Windows/Active Directory asettaa salasanalle tietyt turvallisuuden vähimmäisvaatimukset ja pakottaa salasanan vaihdon sopivin määräajoin, mutta kaikissa muissa järjestelmissä näin ei ole. (Liite 1)

VPN-yhteys sekä External RDP Terminal Server yhdyskäytävät on suojattu Man-In-The-Middle-hyökkäyksiltä käyttäen sertifikaattia johon domainissa olevat koneet luottavat. Tämä suojaus ei päde domainin ulkopuolisille laitteille kuten kotitietokoneille tai puhelimille, eikä suojaa myöskään brute-force-hyökkäyksiltä. FTP-palvelin lukitsee IP-osoitteen väliaikaisesti havaitessaan brute-force-hyökkäyksen. (Asiantuntija X 2018.)

VPN paljastaa internetin yli vain valmistajan (Watchguard). TS Gateway paljastaa valmistajan (Microsoft) ja ohjelmistoversion (IIS 8.0). Langattomista verkoista selviää valmistaja, RADIUS-autentikoidusta langattomasta verkosta selviää sisäverkon domain. PSK-autentikaatiolla suojatut langattomat verkot ovat alttiita dictionary-hyökkäyksille, sillä WPA2/PSK bruteforce-hyökkäystä vastaan ei voi suojautua, koska väsytys ei kohdistu verkkoon, vaan se tehdään offline. (Asiantuntija X 2018.)

Todennuksessa käytettävät tunnistamistiedot (todennuskredentiaalit) suojataan Internetin yli TLS ja/tai OpenVPN teknologioita käyttäen. Esimerkiksi kulunvalvonnan liikenne ei ole suojattua ja siksi se on eristetty omaan virtuaalilähiverkkoon. FTP-palvelimen tunnistustietoja ei ole suojattu mitenkään. TLS ja OpenVPN protokollat suojaavat mahdollisilta uudelleenlähetys-hyökkäyksiltä. Tämä ei koske FTP:tä koska sitä ei suojata muutenkaan. (Asiantuntija X 2018.)

Oletussalasanat tulisi vaihtaa organisaation salasanapolitiikan mukaisiin laadukkaisiin salasanoihin. Työasemissa tämä salasanapolitiikka on pakotettuna, joskin yhteiskäyttötunnuksien salasana on staattinen. Myöskään Local Admin salasanaa ei vaihdeta säännöllisesti ja se on sama jokaisessa työasemassa. Domain admin tasoisten tunnuksien salasanan säännöllistä vaihtoa ei myöskään ole pakoitettu. (Liite 1)

Verkon aktiivilaitteiden, kuten palomuurien, reitittimien, kytkimien, ja langattomia tukiasemien oletussalasanat on vaihdettu, mutta prosesseja ja palveluita ei niin työasemien kuin aktiivilaitteidenkaan kohdalla rajata kuin eritystapauksissa (esimerkiksi erittäin haavoittuvainen telnet-protokolla on estetty). Tämä vaatisi erillisen määrittelyn oleellisten palveluiden tarpeista, eikä sitä nähdä tällä hetkellä tärkeänä. Verkkolaitteiden ohjelmistot pidetään automaattisesti ajan tasalla. (Liite 1)

Verkkolaitteiden hallintayhteys ei ole mahdollista ilman käyttäjän tunnistamista ja todentamista, paitsi työasemien kohdalla yleisillä domain administrator tunnuksilla, joita on käytössä. Hallintayhteyksissä ei käytetä tällä hetkellä aikakatkaisua. (Liite 1)

Palvelimien ja työasemien käyttöjärjestelmiin ja sovellusohjelmistoihin asennetaan tarvittavat turvapäivitykset automaattisesti ja säännöllisesti. Käytössä on verkkoliikenteen vain välttämättömään rajaava (host-based) palomuuriratkaisu. Järjestelmiin asennuksen

yhteydessä automaattisesti luotujen administrator ja guest-tilien oikeuksia ei ole rajattu eikä niitä olla poistettu käytöstä. (Liite 1)

Työasemien lukitus tapahtuu automaattisesti 15 minuutin kuluessa. Median autoplay ja autorun toimintoja ei ole tällä hetkellä estetty. BIOS asetuksiin pääsy vaatii local admin tunnuksen salasanaa. Järjestelmän tukemia lisäturvallisuusominaisuuksia kuten DEP (Data Execution Prevention) tai ASLR (Address space layout randomization) ei tällä hetkellä hyödynnetä, joskin tilanne voi olla eri käyttöjärjestelmäpäivityksen jälkeen. Esimerkiksi Windows 10:n BitLocker suojaus otetaan käyttöön. (Liite 1)

Haittaohjelman torjuntaohjelmistot on asennettu kaikkiin sellaisiin järjestelmiin, jotka ovat alttiita haittaohjelmatartunnoille. Torjuntaohjelmistot ovat toimintakykyisiä ja käynnissä. Torjuntaohjelmistot tuottavat havainnoistaan lokitietoja ja hälytyksiä. Haittaohjelmatunnisteet päivittyvät säännöllisesti. (Liite 1)

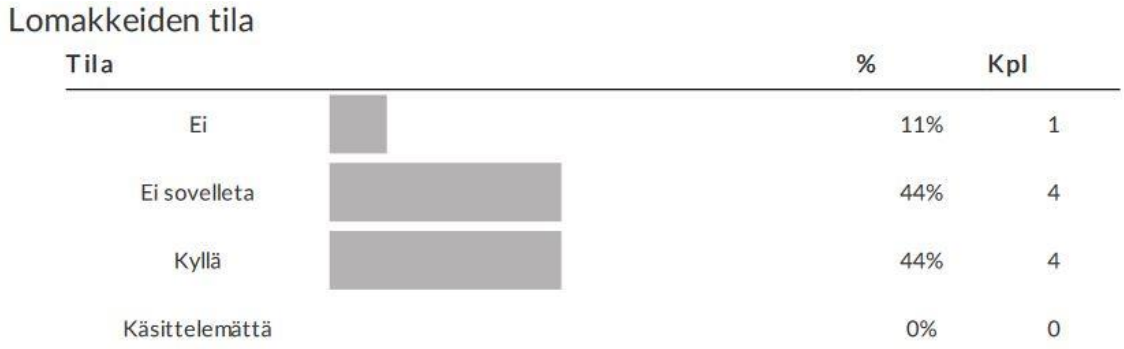
Käyttäjiä on ohjeistettu haittaohjelmauhista ja organisaation tietoturvaperiaatteiden mukaisesta toiminnasta. Haittaohjelmahavaintoja sekä hälytyksiä seurataan säännöllisesti ja niihin reagoidaan. Organisaatiossa suodatetaan haittaliikennettä vähintään sähköpostin ja WWW-liikenteen yhdyskäytävissä (Liite 1). Lokitiedot ja niiden kirjauspalvelut on suojattu luvattomalta käytöltä käyttöoikeuksin, mutta Kaikkia tarvittavia Audit Policy valvontakäytäntöjä ei ole tällä hetkellä käytössä ja tapahtumien säilyvyysaika on auditoinnin perusteella tällä hetkellä liian lyhyt eli alle kuusi kuukautta (Katakri - Tietoturvallisuuden auditointityökalu viranomaisille 2015).

Verkkolaitteiden liikennöintimääriä valvotaan Observium-valvontaohjelmiston kautta ja sen avulla pystytään vertaamaan normaalia ja ongelmatilannetta. Portti- tai ohjelmistotasolla pystytään estämään havaittua haitallista liikennettä. Verkkoliikenteen palomuurissa on tunkeutumisen estämisjärjestelmä (Intrusion Prevention System). (Liite 1)

Yritys ei tarjoa ulkopuolisille rajapintoja palveluihin, sovelluksiin tai tietojärjestelmiin, sillä ainoastaan yrityksen julkinen verkkosivu näkyy verkon ulkopuolelle, eikä siellä ole turvallisuuden kannalta olennaista tietoa. Tietojen luvaton muuttaminen tiedostopalvelimella on estetty käyttöoikeuksin. Tämän lisäksi tiedostopalvelimella on lokitus ja varmuuskopiointi käytössä, joilla tarkistetaan käyttö ja korjataan tarvittaessa. (Liite 1)

4.3 Tietoaineistoturvallisuus

Tietoaineistoturvallisuus osa-alue keskittyy yrityksen tietojen siirtelyyn, tulostukseen, kopiointiin ja hävittämiseen. Korkeamman suojaustason tietojenkäsittelyn vaatimuksia ei tutkimuksessa sovellettu, sillä yrityksen salassa pidettävän tiedon määrä on hyvin vähäinen. Ainut puute oli yrityksen sisäisen verkkoliikenteen salauksen puute.



Kuvio 8: Tietoaineistoturvallisuuden tulokset (Yrityksen riskienhallintatyökalun raportti 2018)

Kun salassa pidettävää aineistoa siirretään fyysisesti suojattujen alueiden ulkopuolella, liikenne salataan TLS-tekniikalla VPN-yhteydessä. Fyysisesti suojattujen alueiden sisäpuolella liikennettä ei ole erikseen suojattu. Fyysisesti suojattujen alueiden ulkopuolella tietoja siirretään vain suojattua VPN-tunnelia hyödyntäen. (Liite 1)

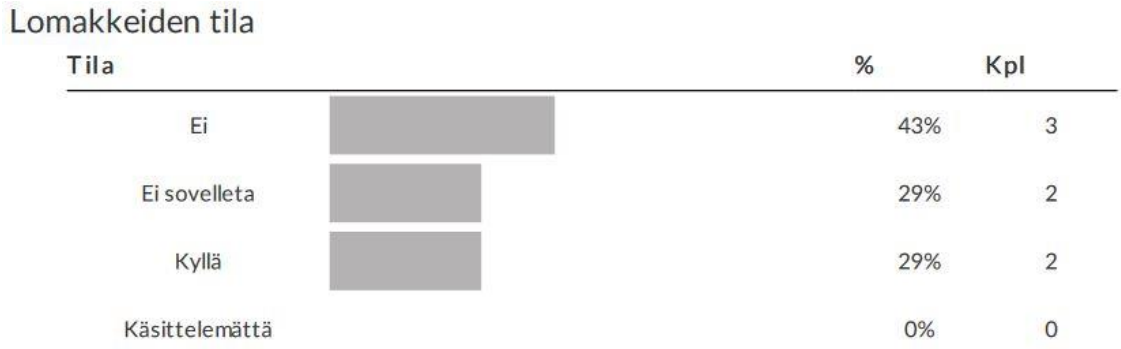
Yksiköiden ja tilojen välillä pyritään siirtämään tietoja vain sähköisiä kanavia pitkin. Kopioiden käsittelyssä noudatetaan alkuperäistä asiakirjaa koskevia turvatoimia. Kopiolaitteiden käyttö on myös estetty ulkopuolisilta. (Liite 1)

Salassa pidettävien tietojen tahallista tai tahatonta vaarantumista tai katoamista valvotaan lokituksen avulla ja estetään käyttöoikeuksin, joskin lokien säilyvyysajan on jo koettu olevan liian pieni. Tietojen säilyvyys varmistetaan varmuuskopioin. (Liite 1)

Yritys on hankkinut ei-sähköisten aineistojen hävittämistä varten palveluna tuhottavat paperiastiat ja niiden tyhjennykset luotettavalta toimijalta. Kiintolevyt tuhotaan luotettavasti, mutta USB-muistien käytöstä ei ole ohjeistettu yrityksen henkilöstöä eikä niiden käyttöä ole estetty. Tilapäiset tiedostot tyhjennetään työasemilta ja tietojärjestelmistä tarpeen mukaan. (Liite 1)

4.4 Käyttöturvallisuus

Käyttöturvallisuusvaatimuksilla varmistetaan, että yrityksen tietoaineistojen käyttö on riittävän turvallista koko niiden elinkaaren ajan. Lisäksi luvussa käsitellään joitakin fyysisen turvan perusvaatimuksia. Soveltamatta jätettiin korkeampien suojaustasojen tietojenkäsittelyä koskevat vaatimukset, koska yrityksellä on hyvin vähän salassa pidettävää tietoa tai niitä käsitellään vähän.



Kuvio 9: Käyttöturvallisuuden tulokset (Yrityksen riskienhallintatyökalun raportti 2018)

Yrityksessä varmistetaan, että järjestelmien ja laitteiden tietoturva on ajan tasalla koko elinkaaren ajan. Konfiguraatioita tiukennetaan tarpeen mukaan. Elinkaaren eri vaiheissa olevat laitteet ovat luetteloituna ja tiedossa (Asset management). (Liite 1)

Turvallisuutta koskevat arvioinnit, tarkastukset ja uudelleentarkastelut suoritetaan poikkeuksellisten tilanteiden ilmetessä. Muutoksia järjestelmiin pystyvät tekemään nimetyt henkilöt, eikä niitä tämän takia tarkasteta määräajoin. Tietojärjestelmädokumentaatiota päivitetään muutoksia tehdessä. (Liite 1)

Muutokset kirjataan tikettijärjestelmään, josta pyynnön tekijä ja muutoksen toteuttaja ovat jäljitettävissä. Muutoksia voi tilata vain yksi henkilö. Muutoksista jää lokiin jälki, joita tarkkaillaan tarvittaessa. (Liite 1)

Näytön sivulta katsomisen suojat ovat käytössä. Vierailijat otetaan vastaan ja kirjataan, mutta kulunvalvontaa tai fyysisiä turvatoimia ei ole kuin osassa rakennusta. Virka-ajan ulkopuolella kulku on rajoitettua ja esimerkiksi tuotannossa koko ajan. (Liite 1)

Ulkoistetun konesalin osalta toimittajilla on asianmukainen ISO/IEC 27001:2013 sertifiointi (IT-Päällikkö 2018). Omissa tiloissa olevien tietojenkäsittelyn osalta keskeisten tilojen (Konesali, sekä IT-tuen huone) on fyysinen lukitus ja avaimet vain rajoitetulla henkilöstöllä. Fyysisesti suojattujen alueiden ulkopuolella tietojenkäsittely on mahdollista vain suojatun VPN-tekniikan avulla. (Liite 1)

Tietoja säilytetään lukituissa ja valvotuissa tiloissa, mutta käyttäjien työasemien osalta tämä ei mahdollista tilaratkaisujen vuoksi. Työasemien tietoja ei myöskään ole salattu, joten mahdollisuus tätä kautta tietoturvauhkaan olemassa. (Liite 1)

Etäkäyttöä varten kannettavissa työasemissa TLS suojattu VPN on käytössä, mutta sen käyttö ei perustu monivaiheiseen tunnistukseen. VPN salasana ei tallennu eikä sitä voi tallentaa clienttiin. VPN käyttää Windows/Active Directory tunnusta ja salasanaa. (Liite 1)

Etäkäytön mahdollistavan VPN clientin asentamisen yhteydessä henkilöä ohjeistetaan suullisesti VPN käytöstä. Kirjallinen ohjeistus uupuu. Työaseman yleisen turvallisen käytön sekä arkaluontoisten tietojen käsittelyn ohjeistukset löytyvät Intranetista. (Liite 1)

Viranomaisten, laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tarpeellisiksi arvioidut turvapäivitykset asennetaan hallitusti, seuranta on ulkoistettu kumppaniyritykselle. Yrityksellä on keskitetty laitehallinta rekisteri, josta tarkistetaan, että laitteet ovat eheät, laitteet ovat verkossa ja että niiden päivitykset ovat ajan tasalla sekä poikkeamien sattuessa käydään tarvittaviin toimiin. (Liite 1)

Yrityksen varmuuskopioinnin taajuus on riittävä menetettävän datan määrään nähden (recovery point objective, RPO). Palautusprosessin nopeus on myös riittävä palautumisen kestoon nähden (recovery time objective, RTO) ja molemmat voidaan tarkistaa tarvittaessa. Toimimattomasta varmuuskopiosta tulee hälytys IT-toimittajalle ja palautusta testataan sovituksen mukaisesti. (Liite 1)

Palautusprosessin dokumentointi on riittävällä tasolla ja opastettu IT-henkilöstölle. Varmuuskopioiden fyysinen sijoituspaikka on eri rakennuksessa ja sijoituksessa on huomioitu mahdollisten sortumien ja tulipalojen riskit. Varmuuskopiot suojataan niiden elinkaaren ajan vähintään vastaavan tasoisilla menetelmillä, kuin millä alkuperäinen tieto. (Liite 1)

5 Riskianalyysi ja tulokset

Riskianalyysin kohteet oli tunnistettu auditoinnilla. Riskianalyysiin otettiin mukaan kaikki tutkimuksen aikana havaitut merkittävät puutteet, joista voisi aiheutua tietoturvariskejä. Kun puutteet olivat selvillä, arvioitiin minkälaisia seurauksia puutteilla voisi olla.

Puutteista esille nousseille riskeille arvioitiin todennäköisyys asteikolla 1-3, joista 1. oli epätodennäköinen, 2. mahdollinen ja 3. todennäköinen. Todennäköisyydeksi arvioitiin todennäköinen, mikäli kohteen valvonta tai ohjeistus on heikkoa, kohteeseen pääsee helposti käsiksi, kohteeseen suuntautuu valtavasti mielenkiintoa, tapahtuma ilmenee vähintään kerran kuukaudessa tai tapahtuma toteutuu suurelle määrälle käyttäjiä. (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003.)

Riskille valittiin mahdollinen todennäköisyys, mikäli kohdetta valvotaan vain osittain, ohjeistus on puutteellista, tapahtuma ilmenee 1-2 kertaa vuodessa tai uhka on mahdollinen tietyille käyttäjäryhmille. Epätodennäköinen valittiin, mikäli kohteen valvonta ja ohjeistus on hyvää ja pääsy rajoitettua, kohteeseen ei suuntaudu mielenkiintoa, tapahtuma ilmenee alle kerran vuodessa tai riskin toteutuminen on mahdollista vain yksittäisille käyttäjille. Seuraavaksi arvioitiin seurausten vakavuus samalla periaatteella, eli 1. vähäinen, 2. haitallinen tai 3. vakava. (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003.)

Seuraukset arvioitiin vakaviksi, jos uhkan toteutuminen aiheuttaa seurauksia kaikille käyttäjille, välittömiä toimenpiteitä, toiminnan keskeytymisen useammaksi tunniksi, suuria taloudellisia kustannuksia, vakavan häiriön organisaation toiminnassa, luottamuksen menetyksen tai raportoinnin viranomaisille ja tiedotusvälineille. Riskille valittiin vakava seuraus, mikäli seurauksilla on vaikutuksia organisaation sisällä tai sen toimintaan, seuraukset koskevat useita käyttäjiä, uhkan toteutuminen aiheuttaa tiedotteen tekemisen tai merkittäviä taloudellisia kuluja. (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003.)

Mikäli uhkan toteutuminen aiheuttaa van sisäisen raportoinnin tai vähäisiä kustannuksia, seuraukset koskevat vain muutamia käyttäjiä tai heidän tietoja, toiminta keskeytyy vain muutamaksi minuutiksi tai seuraukset koskevat vain muutamaa käyttäjää tai heidän tietojaan, niin seuraukset arvioitiin vähäisiksi. Lopuksi riskin suuruus määriteltiin yhdistämällä riskin todennäköisyys ja seurausten vakavuus alla olevan riskitaulukon mukaisesti (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003.):

	Seurausten vakavuus		
Riskin todennäköisyys	1. Vähäinen	2. Haitallinen	3. Vakava
Epätodennäköinen	1. Merkityksetön	2. Vähäinen	3. Kohtalainen
Mahdollinen	2. Vähäinen	3. Kohtalainen	4. Merkittävä
Todennäköinen	3. Kohtalainen	4. Merkittävä	5. Sietämätön

Taulukko 1: Riskitaulukko (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003.)

Riskin todennäköisyydellä ja seurausten vakavuudella on molemmilla kolme eri tasoa. Arvioinnin perusteella valitaan seuraukselle vakavuustaso taulukon ylimmältä riviltä ja tämän jälkeen riskin todennäköisyys ensimmäisestä sarakkeesta. Riskin suuruus määräytyy valittujen tasojen leikkauspisteessä olevan arvon mukaan. (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003.)

Vaaraa aiheuttava puute	Seuraus	Todennäköisyys	Vakavuus	Riskin suuruus
Salausratkaisujen puute	Tietomurto tai -vuoto, maineen menetys, lisäsanktioita EU:lta	2. Mahdollinen	3. Vakava	4. Merkittävä
Lokitietojen säilyvyysajan lyhyys	Tietomurron tai -vuodon huomaamatta jääminen, tietojen ja/tai maineen menetys, mahdollisia lisäsanktioita EU:lta	1. Epätodennäköinen	3. Vakava	3. Kohtalainen
Kulunvalvonnan puutteet	Hyökkääjän pääsy tiloihin, social engineering-hyökkäys, vakoilu, tallennusvälineiden varastaminen	2. Mahdollinen	2. Haitallinen	3. Kohtalainen
Verkkopistokkeiden suojauksen puute	Hyökkääjän pääsy verkkoon	2. Mahdollinen	2. Haitallinen	3. Kohtalainen
Yhteiskäyttötunnukset	Tahaton tietomurto, Social engineering-hyökkäys	2. Mahdollinen	2. Haitallinen	3. Kohtalainen
Puutteet järjestelmäkovennuksessa	Hyökkäys epäturvallisen ohjelman, palvelun tai prosessin kautta	1. Epätodennäköinen	2. Haitallinen	2. Vähäinen
AutoRun ja AutoPlay haavoittuvuudet	Tartutetun median avaaminen USB-muistitikulta tai haitallisen verkkosovelluksen laukaisu	2. Mahdollinen	1. Vähäinen	2. Vähäinen
Etäkäytön puutteet	Hyökkääjän pääsy järjestelmään varastetulla (kannettavalla) työasemalla, tietomurto	1. Epätodennäköinen	2. Haitallinen /1. Vähäinen	2. Vähäinen/ 1. Olematon
Langattomien verkkojen suojauksen puute	Hyökkääjä saapuu verkon reunalle, murtaa suojauksen ja pääsee verkkoon	1. Epätodennäköinen	2. Haitallinen /1. Vähäinen	2. Vähäinen/ 1. Olematon

Taulukko 2: Riskianalyysin tulokset

Salausratkaisujen puute nousi suurimmaksi riskiksi. Kaikkien käyttäjien tiedot ovat salaamattomassa muodossa, joten uhka voi mahdollisesti toteutua suurelle määrälle käyttäjiä. Moni varmasti muistaa vielä miten Sonylle kävi vuonna 2011, kun hyökkääjät saivat käsiinsä miljoonia luottokorttitietoja, kun tietoja ei oltu kryptattu (Arthur, C. & Quinn, B. 2011).

Riskin todennäköisyys arvioitiin kuitenkin vain mahdolliseksi, sillä vaikka potentiaalinen vaikutusalue on laaja, niin pelkkä salauksen puute ei vielä aiheuta tietomurtoa, vaan hyökkääjän on ensin päästävä sisälle järjestelmään, tai saatava fyysinen tallennusväline haltuun. Verkon suojaus on muilta osin varsin hyvällä tasolla, ja yritys tulee korjaamaan tilanteen seuraavan käyttöjärjestelmä päivityksen yhteydessä, kun Windows 10:n BitLocker toiminto otetaan käyttöön.

Oikeaan paikkaan, kuten henkilöstöhallintoon iskenyt hyökkääjä voisi salausratkaisujen puutteen vuoksi onnistuessaan saada käsiinsä sekä salassa pidettävää tietoa, että työntekijöiden henkilötietoa. Mikäli henkilötietoja pääsisi vuotamaan yrityksen ulkopuolelle, EU voi äärimmäisessä tapauksessa määrätä yritykselle sakkoja, jos turvatoimien laiminlyönti on ollut räikyvää. Näin ollen tapauksella olisi valtavia maineellisia ja taloudellisia vaikutuksia, joten seurausten vakavuus arvioitiin vakavaksi.

Verkkopalveluiden, palvelinten ja työasemien kirjautumistietojen lokitiedot ovat keskeisiä tallenteita. Lokia olisi kannattavaa kerätä ainakin järjestelmän toiminnasta, käyttäjäaktiviteeteista, turvaan liittyvistä tapahtumista sekä poikkeamista. Lisäksi verkkolaitteiden lokeista pitäisi tarvittaessa lisäksi selvitä, mitä hallintatoimenpiteitä niille on tehty, kuka on tehnyt ja milloin on tehty. (Kansallinen turvallisuusauditointikriteeristö Katakri 2015.)

Yritys kerää lokia työasemien kirjautumistiedoista, palvelimien käytöstä ja verkkolaitteista, mutta lokien sisällön tarkkuus ei ole riittävä ja säilytysaika on liian lyhyt. Lokitusajan lyhyys ei vielä aiheuta tietomurtoa, mutta voi haitata merkittävästi sen havaitsemista. Lisäksi kun aletaan soveltaa EU:n yleistä tietosuoja-asetusta, yrityksen on tehtävä ilmoitus valvontaviranomaiselle 72 tunnin kuluessa. Mikäli iskua ei havaita, EU voi määrätä yritykselle rangaistuksen (Tietoturvaloukkaukset 2017). Puutteelliset lokitiedot hidastavat reagointia tietomurtoon ja voivat aiheuttaa merkittäviä taloudellisia tai maineellisia vahinkoja yritykselle, joten seurausten vakavuus on arvioitu vakavaksi.

Yleinen käytäntö on, että vieras ilmoittautuu saapuessaan vastaanotosta löytyvään sisäänkirjautumisjärjestelmään, josta yhteyshenkilö saa ilmoituksen ja saapuu ottamaan vieraan vastaan. Ilman henkilökorttia tai saattajaa, koko rakennuksen sisällä liikkuminen on ehdottomasti kielletty. Kaikkia yrityksen työntekijöitä on ohjeistettu puuttumaan epäilyttävään toimintaan.

Näin ei kuitenkaan välttämättä aina tapahdu. Hyökkääjä voisi esimerkiksi teeskennellä yrityksen työntekijää, hämäten puhelimeen puhuen ja näin ollen marssia muina miehinä suoraan liiketiloihin fyysisten turvatoimien puutteiden vuoksi. Riskin todennäköisyys on arvioitu mahdolliseksi, koska valvonnassa on puutteita ohjeistuksesta huolimatta. Se, kuinka paljon aiheutuu vahinkoa, riippuu hyvin pitkälti siitä, kuinka nopeasti välikohtaus havaitaan. Koska tapaus aiheuttaisi todennäköisesti muutoksia yrityksen toimintaan ja vähintään tiedotteen tekemisen, niin seuraus on arvioitu haitalliseksi.

Käyttämättömiä verkkopistokkeita ei myöskään ole suojattu mitenkään ja ne ovat aktiivisia. Jos hyökkääjä pääsisi fyysisesti yrityksen tiloihin sisälle, hän voisi kytkeytyä suoraan yrityksen verkkoon kytkemällä vain laite suoraan vapaaseen verkkopistokkeeseen. Tunkeutumisestojärjestelmä todennäköisesti havaitsisi tällaisen epätavallisen liikenteen ja se voitaisiin mahdollisesti pysäyttää, mutta vahinkoa ehtisi silti mahdollisesti tapahtua. Avoimen verkkopistokkeen löytäminen ja siihen kytkeytyminen on hyökkääjälle mahdollista valvonnan ja fyysisten turvatoimien puutteen vuoksi. Seurausten vakavuus arvioitiin haitallisiksi samoista syistä kuin fyysisen turvan puutteiden kohdalla.

Yhteiskäyttötunnuksilla ongelmaksi nousee se, ettei lokitapahtumia tarkkaillessa voida olla täysin varmoja siitä, kuka tunnusta on sillä hetkellä käyttänyt. Ne ovat myös otollisia kohteita hyökkääjälle, koska niiden salasanoja ei useinkaan vaihdeta ja tietohallintoon soittaessa IT-tukihenkilö ei pysty erityisen hyvin vahvistamaan soittajan henkilöllisyyttä.

Yhteiskäyttötunnuksista aiheutuvien ongelmien uhka arvioitiin mahdolliseksi, sillä uhka rajoittuu tiettyyn käyttäjäryhmään (vuorotyöntekijöihin ja muihin jotka käyttävät ryhmätunnuksia), niiden tilitapahtumia ei voi valvoa lokituksella täydellisesti, tunnusten dokumentaatiossa ja ylläpito-ohjeistuksissa on puutteita sekä yhteiset periaatteet puuttuvat. Seurausten vakavuus riippuu tietomurron laajuudesta, mutta todennäköisesti tapaus aiheuttaisi vähintään muutoksia yhteiskäyttötunnusten käyttäjähallintaan, joten seuraus arvioitiin haitalliseksi.

Järjestelmän koventamisella tarkoitetaan järjestelmän haavoittuvuuspinta-alan pienentämistä oletusasetuksia muuttamalla. Onnettomuuksista, virheistä tai luvattomasta käytöstä johtuvia virheitä rajoitetaan, vaihtamalla oletussalasanat, poistamalla tarpeettomat ohjelmat ja käyttäjätunnukset, sekä antamalla palvelimille, työasemille, verkon aktiivilaitteille ja automaattiprosesseille vain niiden toiminnan kannalta välttämättömät toiminnot ja palvelut. (Kansallinen turvallisuusauditointikriteeristö Katakri 2015.) Tällä hetkellä vain hyvin haavoittuvaiset, kuten Telnet-protokolla on estetty.

Koska järjestelmän kovennusta ei ole juurikaan tehty, hyökkääjälle voi teoriassa tarjoutua takaovi järjestelmään epäturvallisen ohjelmien tai palveluiden kautta. Tätä ei voi kuitenkaan nähdä mitenkään todennäköisenä riskinä. Koska verkon aktiivilaitteeseen kohdistuessa

hyökkäyksellä voisi olla seurauksia verkon toimintaan ja useampiin käyttäjiin, niin seuraukset on arvioitu haitallisiksi.

USB-laitteilla toteutettavat hyökkäykset ovat Mandyn (2010) mukaan varsin yleisiä tänä päivänä paristakin syystä. Ne ohittavat palomuurin ja muut verkonsuojalaitteet kokonaan, voivat pitää sisällään kohtalaisen paljon dataa, ovat halpoja, ja työntekijä on kohtalaisen helposti houkuteltavissa sellaisen kytkemiseksi työasemaan. Käyttöjärjestelmän perusasetuksillakin järjestelmä saattaa käynnistää ohjelman kytketyltä massamuistilaitteelta automaattisesti.

Jotkin verkkosivut voivat vastaavasti käyttää erilaisia Flash ja Java liitännäisiä hyödyntäviä haittaohjelmia verkkopalveluissa, jotka toimivat samalla tavalla, eli kun video tai vastaava media alkaa, ohjelma käynnistää haitallisen koodin joka tartuttaa kyseisen työaseman. Samanlaisia haitallisia koodinpätkiä voidaan upottaa myös PDF-tiedostoon, jolloin haitallinen koodi voi laueta jo esikatseluvaiheessa. Koska USB-muisteista ei ole tällä hetkellä kunnon ohjeistusta, niin uhka arvioitiin mahdolliseksi. Koska uhka rajoittuu todennäköisesti vain yhteen työasemaan ja tilanne on korjattavissa työaseman uudelleen asennuksella ja varmuuskopioiden palautuksella, seuraukset on arvioitu vähäisiksi.

VPN-ohjelmiston turvallisuudessa on joitakin puutteita. Ensinnäkin ohjelmisto ei aikakatkaise itseään, jos järjestelmä on toimettomana kuin tilapäisesti. Yhteys muodostuu uudelleen automaattisesti, kun järjestelmää käytetään taas. Lisäksi yhteyden muodostus kysyy tunnistautumiseen vain tavallista Windows/AD käyttäjätunnusta ja salasanaa.

Jos käyttäjä jättää epähuomiossa työasemansa lukitsematta ja vartioimatta julkisella paikalla tai hyökkääjä saa käsiinsä käyttäjän kirjautumistiedot, niin hyökkääjä pääsisi suoraan käsiksi järjestelmään. Riskin toteutuminen edellyttää, että käyttäjä osoittaa merkittävää huolimattomuutta tai välinpitämättömyyttä turvallisten etätyötapojen suhteen ja näin ollen se on arvioitu epätodennäköiseksi. Seurausten vakavuus riippuu siitä, kuinka paljon salassa pidettävää tietoa käyttäjällä on hallussaan, mutta yleisesti tutkija näkee seurauksen korkeintaan haitallisena.

Langattomien verkkojen, jotka käyttävät PSK-suojattua autentikaatiota suojaus voidaan murtaa dictionary-hyökkäyksille. Hyökkääjä voi kuunnella muita verkon laitteita ja mahdollisesti kaapata toisen käyttäjän istunnon, jos saa verkon salasanan murrettua. Koska verkot on kuitenkin suojattu WPA2/PSK tekniikalla ja langattomien verkkojen kuuluvuutta on pyritty rajoittamaan rakennuksen seinien ulkopuolelle, tapahtuman todennäköisyys on melko epätodennäköinen. Seurausten vakavuuteen voidaan soveltaa samaa arviota, kuin etäyhteyden edellisessä riskissä.

6 Johtopäätökset

Kartoituksen perusteella yrityksen tietojärjestelmiin ei kohdistu välitöntä ulkoista tai sisäistä uhkaa. Tietoturva on yrityksen toimialaan nähden hyvällä tasolla. Salausratkaisuihin on tulossa muutos Windows 10 päivityksen myötä, mutta ennen sitä olisi suotavaa ohjeistaa henkilöstöä tilanteesta. Lokitietojen kohdalla tutkija kehottaa yritystä ryhtymään toimiin riskin pienentämiseksi sopivalla aikajänteellä ja huomioimalla toimenpiteiden kustannukset. Tämän jälkeen sama tulisi tehdä muille riskianalyysin kohtalaisille riskeille. (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003.)

Vähäiset riskit eivät välttämättä vaadi toimenpiteitä, mutta niiden tilannetta kannattaa seurata ja harkita toimenpiteitä, jotka eivät aiheuta turhia kustannuksia. Langattomien verkkojen ja etäkäytön puutteet eivät ole yhtä merkittäviä ja yritys voi halutessaan ohittaa ne. (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003.) Seuraavissa alaluvuissa käydään läpi tutkijan esittämät korjaustoimenpiteet.

6.1 Salausratkaisujen puute

Työasemia tai verkkolevyjä ei ole salattu. Vähintään kaiken verkkolevyillä sijaitsevan henkilötiedon sekä kaikkien kannettavien työasemien kovalevyjen olisi hyvä olla kryptattu asianmukaisella suojauksella. Kannettavilla tietokoneilla on suurempi riski päätyä vääriin käsiin kuin pöytätietokoneilla, jonka lisäksi EU:n tietosuoja-asetus asettaa uusia vaatimuksia henkilötietojen suojaamiseen. Tähän on tosin jo tulossa korjaus tulevan Windows 10 päivityksen ja sen BitLocker toiminnon mukana.

6.2 Turvallisuuteen liittyvien tapahtumien jäljitettävyys

Lokitus on tällä hetkellä päällä, mutta lokien sisällön tarkkuus ei ole riittävä ja säilytysaika on liian lyhyt. Tavoitteeseen pääsemiseksi pitäisi mahdollisesti kytkeä Windowsin valvontakäytännöistä (Audit Policy) ainakin seuraavat onnistuneet ja epäonnistuneet tapahtumat päälle (Kansallinen turvallisuusauditointikriteeristö Katakri 2015):

- Valvo tilien kirjautumistapahtumia (Audit account logon events)
- Valvo tilienhallintaa (Audit account management)
- Valvo kirjautumistapahtumia (Audit logon event)
- Valvo käytäntöjen muutoksia (Audit policy change)
- Valvo oikeuksien käyttöä (Audit privilege use)
- Valvo järjestelmätapahtumia (Audit system events)

Lokien säilytykselle on myös varattava tarpeeksi tilaa ja aikaa, sillä järjestelmä kirjoittaa vanhojen lokitietojen päälle tilan täyttyessä, mikä vähentää säilytysaikaa merkittävästi. Järjestelmälle on syytä varata reilusti ylimääräistä tilaa, sillä tietyt hyökkäystyypit ja poikkeamat kasvattavat siitä syntyvää lokimäärää huomattavasti. Mittaamalla yhden kuukauden aikana kertynyttä lokimäärää voidaan arvioida tarvittavat määritykset halutulle ajanjaksolle, joka olisi parhaassa tapauksessa vähintään kuusi kuukautta. (Kansallinen turvallisuusauditointikriteeristö Katakri 2015.)

6.3 Kulunvalvonnan puutteet

Jo pelkkä kulkulupakortilla suojattu ovi yhdessä vartijan tai vastaanottotyöntekijän kanssa voisi rajata laitonta pääsyä muihin tiloihin huomattavasti. Tehokkaammilla fyysisillä turvatoimilla saataisiin rajattua myös muita riskejä. Esimerkiksi verkkopistokkeiden erilliselle suojaukselle ei olisi tarvetta, jos hyökkääjä ei pääse niihin fyysisesti käsiksi.

6.4 Yhteiskäyttötunnukset

Yhteiskäyttötunnuksia olisi syytä välttää niiden käytöstä johtuvien tunnistus-, todennus-, hallinto- ja tietoturva-ongelmien vuoksi. Niiden salasanoja on hankala vaihtaa määräajoin, sillä tunnusta käyttää useampi käyttäjä. Toimintatapahtumien seuraaminen lokien avulla on myös haastavaa, sillä lokiin ei jää leimaa siitä, kuka tunnusta milloinkin käyttää.

Yhteiskäyttötunnusten käyttö on esimerkiksi tuotantoympäristössä ihan perusteltua, mutta vaatii selkeät ohjeistukset ja menetelmät niiden ylläpidosta. Yhteiskäyttötunnuksilla tulisi voida kirjautua vain erikseen määriteltyihin yhteiskäyttötietokoneiseen, estämällä kirjautuminen esimerkiksi kaikkiin tietokoneisiin, joita ei ole lisätty erilliseen yhteiskäyttöryhmään Active Directoryssa. Näin tunnusten väärinkäyttöä voidaan rajata hieman.

Yhteiskäyttötunnusta luodessa tilille määritetään tunnuksen yhteyshenkilö Active Directoryn Organization-välilehdelle Manager-kenttään, esimerkiksi osaston esimies joka on vastuussa tunnuksen käytöstä ja johon ollaan yhteydessä ongelmatilanteissa. Turvallisuussyistä yhteiskäyttötunnuksilla tulisi aina olla vanhenemispäivä Active Directoryssa, korkeintaan yksi vuosi kerrallaan. Eräpäivän lähestyessä yhteyshenkilö saisi ilmoituksen IT-tuelta, jonne hän ilmoittaa tunnuksen jatkosta tarvittaessa.

Active Directoryn General-välilehden Description-kenttään kuvataan lyhyesti, mihin tunnusta käytetään ja muutoksia tehdessä kaikki tikettinumerot kirjataan Telephones-välilehden Notes-kenttään. Salasana selviää IT-tuelle tarvittaessa tikettinumerosta. Yhteiskäyttötunnuksien pääsyoikeuksien muuttamiseen on suhtauduttava tiukemmin kuin henkilökohtaisten tunnusten kohdalla.

Minkäänlaisia pysyviä adminoikeuksia ei tulisi antaa yhteiskäyttötunnukselle eikä geneerisiä Domain Admin tai Administrator tilejä pitäisi olla käytössä. Jos yhteiskäyttötunnus tai tavallinen käyttäjä jostain syystä tarvitsee joskus adminoikeuksia (esimerkiksi laitteiden tai ohjelmistojen asentamiseen tai tiettyihin asetuksiin käsiksi pääsyyn), tätä varten voidaan luoda Active Directoryyn tilapäisadmin ryhmä, joka tyhjennetään käyttäjistä automaattisesti hakemistopalvelimelta joko komentorivin tai PowerShellin avulla joka päivän päätteeksi.

Tällä hetkellä vain Windows/Active Directory tunnukset menevät lukkoon liian monen epäonnistuneen kirjautumisyrityksen jälkeen. Olisi suositeltavaa, että toiminto otettaisiin käyttöön kaikkien järjestelmien kohdalla, joita IT-tuen on mahdollista hallinnoida. Näin kaikki käyttäjät voidaan suojata mahdollisilta brute-force-hyökkäyksiltä.

6.5 Verkkoporttien suojauksen puute

Lankaverkon verkkoporttien osalta Geier (2014) suosittelee vähintään MAC-osoitteiden suodatuksen ottamista käyttöön. Tämän myötä vain laitteilla, joiden MAC-osoite on erikseen hyväksytty, olisi pääsy verkkoon. Tämä ei todennäköisesti pysäytä määrätietoista hyökkääjää kokonaan, mutta ainakaan työntekijät eivät voi aiheuttaa vaaraa kytkemällä tietämättään omia laitteitaan yrityksen verkkoon.

Jos halutaan varmistaa täydellinen turvallisuus verkkoporttien käytön suhteen, niin muita vaihtoehtoja ovat pistokkeiden lukitseminen fyysisesti, käyttämättömien porttien sulkeminen suoraan kytkimeltä (ei toimi neuvotteluhuoneissa) tai 802.1x porttikohtainen autentikointi. 802.1x protokollassa erillinen varmennuspalvelin estää verkkopalveluiden lähettämisen verkkoon liitetyille laitteille, joilla ei ole vaadittuja tunnistustietoja. Yrityksellä on jo käytössä RADIUS-palvelin, joka voitaisiin määritellä 802.1x protokollassa tarvittavaksi autentikointipalvelimeksi. (Understanding and Configuring 802.1X Port-Based Authentication.)

6.6 Puutteet järjestelmäkovennuksessa

Kaikkien verkon laitteiden palvelut tulisi käydä läpi ja poistaa tarpeettomat käytöstä. Näin saadaan pienennettyä järjestelmien haavoittuvuus pinta-alaa ja monta haavoittuvaa ohjelmaa ja palvelua pois käytöstä. Tarpeettomat verkkopistokkeet ja muut turhat tietoliikenneväylät olisi myös syytä poistaa käytöstä.

Jos verkkotulostimia käytetään salassa pidettävien tietojen käsittelyyn, niitä tulisi myös käsitellä verkon aktiivilaitteina (Puolustusministeriö, 2015). Tämä koskee oletussalasanojen vaihtoa, tarpeettomien verkkopalveluiden estämistä ja turhien verkkopistokkeiden poistamista käytöstä. Yrityksellä on käytössä menetelmät asian korjaamiseksi, mutta resurssit uupuvat, eikä työmäärästä johtuen asiaa nähdä tällä hetkellä tärkeänä.

6.7 AutoRun ja AutoPlay haavoittuvuudet

AutoRun ja autoplay ominaisuudet olisi syytä kytkeä pois päältä ja PDF lukuohjelman Protected Mode päälle, mieluiten jo järjestelmän asennus vaiheessa, jolloin saadaan aikaan kovennettu asennus. Jotkut, esimerkiksi ulkomaiset patentti- ja lääkeyritykset joutuvat levittämään erittäin salaisia dokumentteja asiakkailleen salatuilla USB-tikuilla, jossa sijaitsee myös tarvittava ohjelma kyseisen dokumentin avaamiseksi. Tällöin IT-tuki voi määrittää tarvittavat asetukset kyseisellä työasemalla sopiviksi. USB-muisteista olisi myös kannattavaa tehdä henkilöstölle ohjeistus.

6.8 Etäkäytön puutteet

VPN-yhteyden avaamisen olisi hyvä käyttää monivaiheista tunnistusta. Paras ratkaisu olisi palvelu, joka kysyy sekä käyttäjätunnusta että salasanaa, mutta myös turvakoodia, joka lähetettäisiin käyttäjän työpuhelimeen aina VPN yhteyttä muodostaessa. Näin estetään hyökkääjän kytkeytyminen verkkoon varastetulla työasemalla, ellei hyökkääjällä ole hallussa myös kohdehenkilön työpuhelin. VPN-yhteydessä olisi suotavaa käyttää aikakatkaisua, joka vaatisi myös uudelleen kirjautumisen, kun yhteys on ollut toimettomana yli 10 minuuttia.

7 Arviointi

Alkuperäiseen suunnitelmaan kuului teemahaastatteluita ja kattavaa dokumenttien läpikäyntiä, mutta opinnäytetyön tekijällä ollut pääsyä kaikkiin järjestelmiin ja dokumentaatiota oli alussa hyvin vähän. Tulkinnanvaraisen auditointikriteeristön ja dokumenttien puutteen takia tutkimuksen painopiste vaihtui palavereihin ja riskienhallintatyökaluun kirjattuihin muistiinpanoihin. Tutkimusaineisto tuli siis suurimmaksi osaksi ainoastaan yhdestä lähteestä eli haastatteluilla.

Palaverit kestivät usein pitkään, jopa yhden työpäivän verran ja niitä oli kolme kaiken kaikkiaan, mutta ne olivat todella tuottoisia. Myös henkilöstön suhtautuminen näihin palavereihin, Katakri viitekehykseen ja koko kartoitusprosessiin oli todella myönteistä ja muutenkin vastaanotto yrityksen puolelta oli joka kerta todella hyvä. Myös korjausehdotukset otettiin kiitollisesti vastaan ja toimeksiantaja arvosti niitä.

Opinnäytetyön tavoitteita olivat nykytilan selvitys, dokumentointi ja korjausehdotusten laatiminen. Mielestäni kaikki tavoitteet täyttyivät ja tutkimuksessa käytetyt menetelmät olivat tutkimuksen kannalta toimivia. Selvitys kattoi koko Katakrin teknisen osion mittakaavan, auditoinnin tulokset on dokumentoitu sekä riskienhallintatyökaluun, että erilliseen raporttiin. Ehdotettuja toimenpiteitä ei valitettavasti päästy testaamaan käytännössä, mutta toimeksiantaja arvioi ne toimiviksi.

Toimeksiantaja arvioi tuotosta sen analyyttisellä ja laadulla ja antoi hyvää palautetta. Sisältöä tuli laadittua jopa laajemmin ja analyyttisemmin, kuin toimeksiantaja oli osannut

odottaa. Korjausehdotukset olivat toimeksiantajan mielestä toimivia ja kuvattu tarpeeksi kattavasti, jotta niiden toimeenpaneminen olisi helppoa.

8 Pohdinta

Opin tutkimuksen aikana huomattavasti uusia asioita. Ensinnäkin kyseessä oli ensimmäinen auditointi, jota olin mukana toteuttamassa. Tietoperustan laatimisessa kesti kohtalaisen kauan, mutta sain aivan uudenlaisia näkökulmia tieteellisten tutkimusten toteuttamiseen. Samalla kirjalliseen materiaaliin perustuva kirjoitustyö tuli todella tutuksi.

Alkuperäinen lähestymistapa dokumenteilla ja kattavilla teemahaastatteluilla olisi ollut mielenkiintoinen ja mahdollisesti tuottavampi, mutta samalla siitä olisi syntynyt vieläkin enemmän työmäärää. Katakrin toista versiota olisi voitu harkita hetki kauemmin. Jos joutuisin tekemään tutkimuksen uudestaan, käyttäisin todennäköisesti toista versiota ensimmäisessä auditoinnissani. Nyt jouduttiin käyttämään huomattavan paljon aikaa oikean tulkitsemistavan miettimiseksi, kun tarjolla olisi ollut virtaviivainen ja yksinkertaisempi vaihtoehto.

Koska tutkijalla ei ollut pääsyä tikettijärjestelmään ja dokumentaatiota oli muutenkin vähän, kaikki tutkimusaineisto oli haastatteluiden varassa. Uhkana on, että haastattelijat myötäilivät tutkijaa liikaa tarkastuksen aikana, antaen sellaisia vastauksia, joita haluttiin kuulla. Tutkimuksen tarkoituksena oli kuitenkin yrityksen oma etu, joten on hankala nähdä syytä sille, että joku ei olisi ollut rehellinen tutkimuksen aikana.

Työelämässä olisi ollut vielä syytä tehdä uusi tarkastus, kun ensimmäisellä kerralla auditoinnissa havaitut puutteet on korjattu. Olisi ollut mielenkiintoista nähdä, miten ehdotetut toimenpiteet vaikuttavat käytännössä. Havaitut puutteet on joka tapauksessa dokumentoitu ja luovutettu toimeksiantajalle, joten yritys voi tehdä niillä, kuten parhaaksi näkee.

Lähteet

Painetut

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 15. painos. Helsinki: Tammi.

Kananen, J. 2013. Case-tutkimus opinnäytetyönä. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Yin, Robert K. 2009. Case Study Research, Design and Methods. 4. painos. Thousand Oaks, CA: SAGE Publications.

Sähköiset

American Society for Quality. 2018. What is auditing? Viitattu 23.5.2018. http://asq.org/learn-about-quality/auditing/

Arthur, C & Quinn, B. 2011. PlayStation Network hackers access data of 77 million users. Viitattu 25.5.2018. https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data

Cisco. Understanding and Configuring 802.1X Port-Based Authentication. Viitattu 26.5.2018. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25sg/configuration/guide/conf/dot1x.pdf

Cochran, C. 2016. Techniques for Gathering Audit Evidence. Viitattu 23.5.2018. http://www.theauditoronline.com/techniques-for-gathering-evidence/

Geier, E. 2014. 8 ways to improve wired network security. Viitattu 16.5.2018. https://www.networkworld.com/article/2175048/wireless/8-ways-to-improve-wired-network-security.html

ISACA. 2014. IS Audit and Assurance Guideline 2205 Evidence. Viitattu 23.5.2018. http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2205-Evidence_gui_Eng_0614.pdf

Sosiaali- ja terveysministeriö, Työsuojeluosasto, Työturvallisuuskeskus. 2015. Riskien arviointi työpaikalla –työkirja. Viitattu 24.5.2018. https://ttk.fi/files/2941/Riskien_arviointi_tyopaikalla_tyokirja_22052015_kerttuli.pdf

Puolustusministeriö. 2011. KATAKRI Kansallinen turvallisuusauditointikriteeristö. Versio II. Viitattu 22.5.2018. http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf

Puolustusministeriö. 2015. Katakri 2015 - Tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 3.5.2018. https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Mandy, D. 2010 Top 10 vulnerabilities inside the network. Viitattu 16.5.2018. https://www.networkworld.com/article/2193965/tech-primers/top-10-vulnerabilities-inside-the-network.html

Tietosuojavaltuutetun toimisto. 2012. Laadi tietotilinpäätös. Viitattu 3.5.2018. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfpzNVCh/Laadi_tietotilinpaatos.pdf

Tietosuojavaltuutetun toimisto. 2013. Tietosuoja-aiheista sanastoa. Viitattu 23.3.2018. http://www.tietosuoja.fi/fi/index/sanasto.html

Tietosuojavaltuutetun toimisto. 2017. Tietoturvaloukkaukset. Viitattu 25.5.2018. https://tietosuoja.fi/fi/tietoturvaloukkaukset

Tietosuojavaltuutetun toimisto. 2018. EU:n tietosuojauudistus. Viitattu 23.5.2018. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html

Valtiovarainministeriö. 2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Viitattu 24.5.2018. https://www.vahtiohje.fi/c/document_library/get_file?uuid=d1bcc4b1-789e-4ce1-a44a-e591a60985b5&groupId=10229

Viestintävirasto. 2013. Sähkömagneettisen hajasäteilyn aiheuttama tietoturvariskien ehkäisyn periaatteet. Viitattu 25.5.2018. https://www.viestintavirasto.fi/attachments/Kansallinen_TEMPEST-ohje.pdf

Julkaisemattomat

Asiantuntija X. Yrityksen looginen verkko 2018-01-25. S-posti. 25.1.2018. Viitattu 25.5.2018.

Asiantuntija X. Re: Kysymys Liittyen tietoturva auditointiin. S-posti. 26.4.2018. Viitattu 26.6. 2018.

IT-Päällikkö. Konesali ISO Serti. S-posti. 17.5.2018. Viitattu 25.5.2018.

Yritys X. Yrityksen riskienhallintatyökalun raportti. 2018.

Kuviot

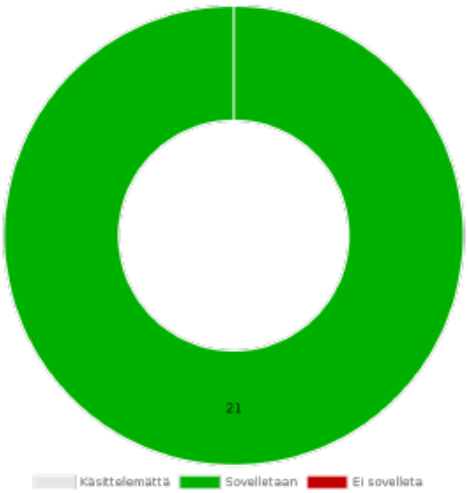
Taulukot

Liitteet

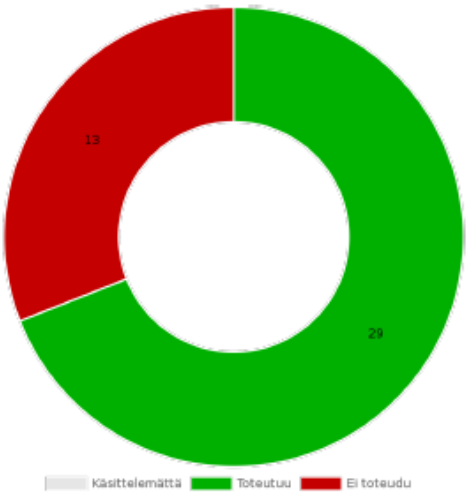
Liite 1: Yrityksen riskienhallintaraportti

Jakaumat

Sovelletaan



Vaatimuslomake: Tila



Lomakkeet

Yhteenveto

Kriteeri	ST.	Sovelletaan	Toteutuu	Päivitetty
I 02 Tietoliikenneverkon vyöhykkeistä- minen ja suodatussäännöstöt ko. suojaustason sisällä	IV-II	Sovelletaan	Kyllä	26.05.2018
I 03 Suodatus- ja valvontajärjestelmien hallinnointi	IV-II	Sovelletaan	Ei	21.05.2018
I 04 Hallintayhteydet	IV-II	Sovelletaan	Kyllä	21.05.2018
I 06 Pääsyoikeuksien hallinnointi	IV-II	Sovelletaan	Ei	21.05.2018
I 07 Tietojenkäsittelyympäristön toimijoiden tunnistaminen fyysisesti suojatun alueen sisällä	IV-II	Sovelletaan	Ei	21.05.2018
I 08 Järjestelmäkovennus	IV-II	Sovelletaan	Ei	21.05.2018
I 09 Haittaohjelmasuojaus	IV-II	Sovelletaan	Kyllä	22.05.2018
I 10 Turvallisuuteen liittyvien tapahtumien jäljitettävyys	IV-II	Sovelletaan	Ei	25.01.2018
I 11 Poikkeamien havainnointikyky ja toipuminen	IV-II	Sovelletaan	Kyllä	25.01.2018
I 12 Salausratkaisut	IV-II	Sovelletaan	Ei	21.05.2018
I 13 Ohjelmistoilla toteutettavat pääsynhallintatoteutukset	IV-II	Sovelletaan	Ei	21.05.2018
I 15 Aineiston sähköinen välitys	IV-II	Sovelletaan	Ei	26.05.2018
I 16 Aineiston välitys postilla ja kuriirilla	IV-II	Sovelletaan	Kyllä	07.03.2018
I 17 Tulostus ja kopiointi	IV-III	Sovelletaan	Kyllä	07.03.2018
I 18 Turvallisuustarkoituksia varten tapahtuva salassa pidettävien tietojen kirjaaminen	IV	Sovelletaan	Kyllä	21.05.2018
I 19 Salassa pidettävää tietoa sisältävien tietoaineistojen hävittäminen	IV	Sovelletaan	Kyllä	22.05.2018
I 20 Muutoshallintamenettelyt	IV-II	Sovelletaan	Ei	21.05.2018
I 21 Fyysinen turvallisuus	IV	Sovelletaan	Ei	22.05.2018
I 22 Etäkäyttö ja etähallinta	IV	Sovelletaan	Ei	22.05.2018
I 23 Ohjelmistohaavoittuvuuksien hallinta	IV-II	Sovelletaan	Kyllä	07.03.2018
I 24 Varmuuskopiointi	IV-II	Sovelletaan	Kyllä	07.03.2018

Yksittäiset lomakkeet

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.1. Tietoliikenneturvallisuus
Kriteeri: I 02 Tietoliikenneverkon vyöhykkeistä- minen ja suodatussäännöstöt ko. suojaustason sisällä
Suojaustaso: IV-II
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt on toteutettava vähimpien oikeuksien (least privilege) ja monitasoisen suojaamisen (defence in depth) periaatteiden mukaisesti.	Toteutuu	Ei ole vyöhykkeistetty tai suodatettu, mutta kaikki ulkopuolelta tuleva liikenne on oletuksena estetty ja sallittu vain tarvittava.	Lindroos Robin	25.05.2018

Toteutuu: Kyllä
Muistiinpanot:
Omistaja:
Lisätietoja: I02.pdf
Liitteet:
Luotu: 19.12.2017 Automaattisesti luotu lomake
Päivitetty: 26.05.2018 Lindroos Robin

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.1. Tietoliikenneturvallisuus
Kriteeri: I 03 Suodatus- ja valvontajärjestelmien hallinnointi
Suojaustaso: IV-II
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
1) Suodatus- ja valvontajärjestelmien tarkoituksenmukaisesta toiminnasta huolehditaan koko tietojenkäsittely-ympäristön elinkaaren ajan.	Toteutuu	Laitteistoilla ja niihin liittyvillä ohjelmistoilla on toimittajan tuki ja niitä valvotaan ja huolletaan.		25.01.2018
2) Liikennettä suodattavien tai valvovien järjestelmien asetusten lisääminen, muuttaminen ja poistaminen on vastuutettu ja organisoitu	Toteutuu	Ainoastaan nimetyillä henkilöillä on oikeudet tehdä muutoksia. Muutos/poisto pyynnöt tulevat keskitetysti.		25.01.2018
3) Verkon ja siihen liittyvien suodatus- ja valvontajärjestelmien dokumentaatiota ylläpidetään sen elinkaaren aikana erottamattomana osana muutosten ja asetusten hallintaprosessia.	Ei toteudu	Järjestelmistä ei ole erillistä dokumentaatiota. Muutosprosessissa ei ole erillistä dokumentaatiota. Muutospyynnöt kirjataan toimittajan tikettijärjestelmään.	Lindroos Robin	23.03.2018
4) Liikennettä suodattavien tai valvovien järjestelmien asetukset ja haluttu toiminta tarkastetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä.	Toteutuu	Muutosmäärät ovat niin vähäisiä, että on todettu niiden olevan tarpeetonta tarkastaa määräajoin. Jokainen muutos tarkastetaan käyttöönottohetkellä.	Lindroos Robin	21.05.2018

Toteutuu: Ei
Muistiinpanot:
Omistaja:
Lisätietoja: I03.pdf

Liitteet:
Luotu: 19.12.2017 Automaattisesti luotu lomake
Päivitetty: 21.05.2018 Lindroos Robin

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.1. Tietoliikenneturvallisuus
Kriteeri: I 04 Hallintayhteydet
Suojaustaso: IV-II
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
1) Hallintayhteydet on rajattu suojaustasoittain, ellei käytössä ole viranomaisen ko. suojaustasoille hyväksymää yhdyskäytäväratkaisua.	Toteutuu	Hallintoyhteydet on rajattu sisäverkkoon ja käyttöoikeudet annettu vain nimetyille henkilöille. Ulkopuoliset toimijat jotka tarvitsevat hallintoyhteyksiä käyttävät VPN:ää ja heillä on käyttöoikeudet vain hallinnoimiinsa järjestelmiin.	Lindroos Robin	21.05.2018
2) Hallintaliikenteen sisältäessä salassa pidettävää tietoa ja kulkiessa matalamman suojaustason ympäristön kautta, salassa pidettävät tiedot on salattu viranomaisen hyväksymällä salaustuotteella.	Toteutuu	Käytössä ei ole kuin yksi suojaustaso.		21.05.2018
3) Hallintaliikenteen kulkiessa ko. suojaustason sisällä, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella viranomaisen erillishyväksyntään perustuen.	Toteutuu	Käytössä ei ole kuin yksi suojaustaso.		21.05.2018
4) Hallintayhteydet on rajattu vähimpien oikeuksien periaatteen mukaisesti.	Toteutuu	Vain rajatuilla henkilöillä on käyttöoikeudet.		25.01.2018

Toteutuu: Kyllä
Muistiinpanot:
Omistaja:
Lisätietoja: I04.pdf
Liitteet:
Luotu: 19.12.2017 Automaattisesti luotu lomake
Päivitetty: 21.05.2018 Lindroos Robin

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.2. Tietojärjestelmäturvallisuus
Kriteeri: I 06 Pääsyoikeuksien hallinnointi
Suojaustaso: IV-II
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
1) Tietojenkäsittely-ympäristön käyttäjille ja automaattisille prosesseille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä.	Ei toteudu	Domain user -tason käyttäjien kohdalla tilanne on kunnossa. Automaattiprosessien ja järjestelmänvalvojien tilannetta olisi syytä tarkastella.	Lindroos Robin	21.05.2018
2) Salassa pidettävien tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely estetään käyttöoikeushallinnan sekä tietojärjestelmien asianmukaisilla turvallisuusjärjestelyillä ja muilla toimenpiteillä.	Toteutuu	Järjestelmissä ja verkkolevyillä oleva tieto on suojattu käyttöoikeuksin.		25.01.2018

Toteutuu: Ei
Muistiinpanot:
Omistaja:
Lisätietoja: I06.pdf
Liitteet:
Luotu: 19.12.2017 Automaattisesti luotu lomake
Päivitetty: 21.05.2018 Lindroos Robin

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.2. Tietojärjestelmäturvallisuus
Kriteeri: I 07 Tietojenkäsittelyympäristön toimijoiden tunnistaminen fyysisesti suojatun alueen sisällä
Suojaustaso: IV-II
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät tietojenkäsittely-ympäristön toimijoiden tunnistamiseen.	Ei toteudu	1. Käytössä on yksilölliset henkilökohtaiset käyttäjätunnisteet. - Vain osittain (käytössä yhteiskäyttötunnuksia) 2. Kaikki käyttäjät tunnistetaan ja todennetaan. -Vain osittain (käytössä yhteiskäyttötunnuksia) 3. Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestetty luotettavasti. -Vain osittain. 4. Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin aiheuttaa tunnuksen lukittumisen. -Vain osassa järjestelmiä. 5. Järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia. Mikäli tämä ei kaikissa järjestelmissä/sovelluksissa ole teknisesti mahdollista, vaaditaan sovitut ja dokumentoidut salasanojen hallintakäytännöt yhteiskäyttöisille tunnuksille. -Vain osittain. 6. Todennus tehdään vähintään salasanaa käyttäen. Mikäli käytetään salasanatodennusta, a) käyttäjiä on ohjeistettu hyvästä turvallisuuskäytännöstä salasanan valinnassa ja käytössä, b) käyttöä valvova ohjelmisto asettaa salasanalle tietyt turvallisuuden vähimmäisvaatimukset ja pakottaa salasanan vaihdon sopivin määräajoin. -Vain osassa järjestelmiä.	Lindroos Robin	21.05.2018

Toteutuu: Ei
Muistiinpanot:
Omistaja:
Lisätietoja: I07.pdf
Liitteet:
Luotu: 19.12.2017 Automaattisesti luotu lomake
Päivitetty: 21.05.2018 Lindroos Robin

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.2. Tietojärjestelmäturvallisuus
Kriteeri: I 08 Järjestelmäkovennus
Suojaustaso: IV-II
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
3) Kovennettu asennus sisältää vain sellaiset komponentit ja palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toimintavaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi.	Ei toteudu	Oletussalasanat vaihdetaan, mutta prosesseja ja palveluita ei rajata kuin eritystapauksissa.	Lindroos Robin	21.05.2018
2) Käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus.	Toteutuu	Menettelytapa on olemassa.	Lindroos Robin	21.05.2018
1) Käyttöön on otettu vain käyttövaatimusten ja tietojen käsittelyn kannalta olennaiset toiminnot, laitteet ja palvelut.	Ei toteudu	Vaatii erillisen määrittelyn oleellisista tarpeista.		25.01.2018

Toteutuu: Ei
Muistiinpanot:

1. Oletussalasanat on vaihdettu organisaation salasanapolitiikan mukaisiin laadukkaisiin salasanoihin.
- Työasemissa on salasanapolitiikka pakotettuna (HUOM, yhteiskäyttötunnuksien salasana on staattinen)
- Local Admin salasanaa ei vaihdeta säännöllisesti. Sama jokaisessa työasemassa.
- Domain admin tasoisten tunnuksien salasanan säännöllistä vaihtoa ei ole pakoitettu

2. Vain tarpeellisia verkkopalveluita on päällä ja nämä palvelut on rajattu vain tarpeellisiin verkkoliittymiin.
3. Verkkolaitteiden ohjelmistoihin on asennettu tarpeelliset turvapäivitykset.
4. Hallinta ei ole mahdollista ilman käyttäjän tunnistamista ja todentamista.
- Kyllä, paitsi Domain administrator tunnus joka käytössä.

5. Hallintayhteyksissä tulisi käyttää istuntojen aikakatkaisua.
- Ei käytössä

6. Kovennukset pohjautuvat johonkin luotettavaksi arvioituun kovennusohjeeseen tai suositukseen.
Palvelimet, työasemat ja vastaavat
-On käytössä mutta perustuu "best practises" malliin

7. Tarjottavat (erityisesti verkko)palvelut on minimoitu ja rajattu vain välttämättömiin. On lisäksi käytössä verkkoliikenteen vain välttämättömään rajaava (host-based) palomuuriratkaisu.
8. Alusta sisältää vain järjestelmän tarvitsemia ohjelmistokomponentteja. Alustan komponenttien, prosessien (esim. palvelinprosessit), hakemistojen ja lisäohjelmien käyttöoikeudet on asetettu tarkoituksenmukaisiksi vähimpien oikeuksien periaatteen mukaisesti.
9. Käyttöjärjestelmään ja sovellusohjelmistoihin on asennettu tarpeelliset turvapäivitykset.
- Kyllä säännöllisesti / automaattisesti

10. Järjestelmiin asennuksen yhteydessä automaattisesti luoduille tileille (esim. "administrator" ja "guest") on oikeudet rajattu minimiin tai poistettu

käytöstä.
- Ei

11. Oletussalasanat on vaihdettu organisaation salasanapolitiikan mukaisiin laadukkaisiin salasanoihin.

12. Järjestelmä lukittuu automaattisesti, jos sitä ei käytetä vähään aikaan (esim. salasanasuojattu näytönsäästäjä aktivoituu 15 minuutin käyttämättömyyden jälkeen).
- Pitää tarkastaa?

13. Käyttöoikeudet asetettu vähimpien oikeuksien periaatteen mukaisesti (vrt. I 06).
14. Käyttöjärjestelmän tunnettuja turvallisuusuhkia sisältävät automaattisen ohjelmakoodin suorituksen mahdollistavat ominaisuudet on kytketty pois päältä (erityisesti PDF-tiedostojen automaattinen esikatselu sekä "autorun" ja "autoplay"-toiminnallisuudet, sekä esimerkiksi USB- ja Firewire-laitteiden automaattisen käynnistymisen estäminen koneen ollessa lukittuna).
- ?

15. Ohjelmistot, erityisesti web-selaimet, PDF-lukijat, toimisto-ohjelmistot ja sähköpostiohjelmistot, ovat turvallisesti konfiguroituja. Ohjelmistojen kovennuksissa tulisi huomioida erityisesti ajettavan koodin (esim. JavaScript sekä makrot) oletusarvoisen suorittamisen estäminen.
- Kyllä. "best practises" mukaisesti

16. BIOS-asetuksiin pääsy on suojattu salasanalla (suojaustasolla IV erityisesti Naton turvallisuusluokitellun tiedon osalta)
- Pitää tarkistaa?

17. Järjestelmän tukemia lisäturvallisuusominaisuuksia (esimerkiksi DEP/ASLR/Applocker/SELINUX) hyödynnetään.
- Ei

Omistaja:

Lisätietoja: I08.pdf

Liitteet:

Luotu: 19.12.2017 Automaattisesti luotu lomake

Päivitetty: 21.05.2018 Lindroos Robin

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.2. Tietojärjestelmäturvallisuus
Kriteeri: I 09 Haittaohjelmasuojaus
Suojaustaso: IV-II
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn estämiseksi tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät haittaohjelmauhkien ennaltaehkäisyyn, estämiseen, havaitsemiseen, vastustuskykyyn ja tilanteen korjaamiseen.	Toteutuu	1. Haittaohjelmantorjuntaohjelmistot on asennettu kaikkiin sellaisiin järjestelmiin, jotka ovat alttiita haittaohjelmatartunnoille. 2. Torjuntaohjelmistot ovat toimintakykyisiä ja käynnissä. 3. Torjuntaohjelmistot tuottavat havainnoistaan lokitietoja ja hälytyksiä. 4. Haittaohjelmatunnisteet (ja vast.) päivittyvät säännöllisesti. 5. Käyttäjiä on ohjeistettu haittaohjelmauhista ja organisaation tietoturvaperiaatteiden mukaisesta toiminnasta. 6. Haittaohjelmahavaintoja sekä hälytyksiä seurataan säännöllisesti ja niihin reagoidaan. 7. Organisaatiossa suodatetaan haittaliikennettä vähintään sähköpostin ja WWW-liikenteen yhdyskäytävissä.		21.05.2018

Toteutuu: Kyllä
Muistiinpanot:
Omistaja:
Lisätietoja: I09.pdf
Liitteet:

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.2. Tietojärjestelmäturvallisuus
Kriteeri: I 10 Turvallisuuteen liittyvien tapahtumien jäljitettävyys
Suojaustaso: IV-II
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn havaitsemiseksi tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät turvallisuuteen liittyvien tapahtumien jäljitettävyyteen.	Ei toteudu	Lokien sisällön tarkkuus ei ole riittävä ja säilytysaika on liian lyhyt. Lokitiedostot on suojattu käyttöoikeuksin.		25.01.2018

Toteutuu: Ei
Muistiinpanot:
Omistaja:
Lisätietoja: I10.pdf
Liitteet:
Luotu: 19.12.2017 Automaattisesti luotu lomake
Päivitetty: 25.01.2018 Lindroos Robin

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.2. Tietojärjestelmäturvallisuus
Kriteeri: I 11 Poikkeamien havainnointikyky ja toipuminen
Suojaustaso: IV-II
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät, joilla pyritään havaitsemaan hyökkäys tietojenkäsittely-ympäristöä vastaan, rajoittamaan hyökkäyksen vaikutukset mahdollisimman pieneen osaan tietoja tai tietojenkäsittely-ympäristön resursseja ja estämään muut vahingot, sekä palauttamaan tietojenkäsittely ympäristön suojattu tilanne.	Toteutuu	Verkkolaitteiden liikennöintimääriä valvotaan (Observium) ja niiden avulla pystytään verrata normaalia ja ongelmatilannetta. Portti- tai ohjelmistotasolla pystytään estämään haitallista liikennettä. Verkkoliikenteen palomuurissa on tunkeutumisen estämisjärjestelmä (IPS).		25.01.2018

Toteutuu: Kyllä
Muistiinpanot:
Omistaja:
Lisätietoja: I11.pdf
Liitteet:
Luotu: 19.12.2017 Automaattisesti luotu lomake
Päivitetty: 25.01.2018 Lindroos Robin

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.2. Tietojärjestelmäturvallisuus
Kriteeri: I 12 Salausratkaisut
Suojaustaso: IV-II
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
Viranomainen on hyväksynyt käytetyt salausratkaisut (ja -tuotteet) ko. suojaustasolle ko. käyttöympäristössä salassa pidettävien tietojen luvattoman paljastumisen ja muuntelun estämiseksi.	Ei toteudu	Tällä hetkellä ei ole käytössä työasemilla eikä palvelimilla.		25.04.2018

Toteutuu: Ei
Muistiinpanot: Tällä hetkellä ei ole käytössä työasemilla eikä palvelimilla.
Omistaja:
Lisätietoja:
Liitteet:
Luotu: 19.12.2017 Automaattisesti luotu lomake
Päivitetty: 21.05.2018 Lindroos Robin

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.2. Tietojärjestelmäturvallisuus
Kriteeri: I 13 Ohjelmistoilla toteutettavat pääsynhallintatoteutukset
Suojaustaso: IV-II
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
1) Tietojenkäsittely-ympäristön turvallisuus, myös niiden tekniset ja muut kuin tekniset turvatoimet, testataan hyväksymisprosessin aikana sen varmistamiseksi, että asianmukainen turvaamistaso saavutetaan, ja sen tarkistamiseksi, että ne on moitteettomasti toteutettu, integroitu ja konfiguroitu.	Ei toteudu	Ei testata, mutta tarvittaessa voidaan palata aiempaan kokoonpanoon.		21.05.2018
2) Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn estämiseksi ja havaitsemiseksi tietojenkäsittely-ympäristössä järjestetään luotettavat menettelyt ohjelmistoilla toteutettavien pääsynhallintatoteutusten turvallisuudesta varmistumiseksi.	Toteutuu	Tiedostopalvelimilla on lokitus käytössä ja tarkistetaan tarvittaessa. Luvaton muuttaminen on käyttöoikeuksilla rajoitettu.		21.05.2018

Toteutuu: Ei
Muistiinpanot:
1. Palvelun/sovelluksen/järjestelmän toteutukselle edellytetään turvallisen ohjelmoinnin periaatteiden täyttämistä, ja toimittajilta vaaditaan selvitys, miten turvallisen ohjelmoinnin periaatteet on käytännössä huomioitu tuotekehityksessä; -Ei edellytetä.
2. Palvelun/sovelluksen/järjestelmän toimittaja sitoutetaan turvallisuuspuutteiden korjaamiseen palvelun/sovelluksen elinkaaren ajalle, tai on olemassa jokin muu menettely, jolla havaitut turvallisuuspuutteet pystytään korjaamaan - Tällä hetkellä ei sitouduteta.
3. Palvelun/sovelluksen/järjestelmän rajapintojen on kestettävä yleiset hyökkäysmenetelmät ilman, että palvelussa/sovelluksessa käsiteltävien salassa pidettävien tietojen luottamuksellisuus tai eheys vaarantuu. - Ulkopuolisille ei tarjota rajapintoja tietojärjestelmiin.
Omistaja:
Lisätietoja: I13.pdf
Liitteet:
Luotu: 19.12.2017 Automaattisesti luotu lomake
Päivitetty: 21.05.2018 Lindroos Robin

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.3. Tietoaineistoturvallisuus
Kriteeri: I 15 Aineiston sähköinen välitys
Suojaustaso: IV-II
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
1) Kun salassa pidettävää aineistoa siirretään hyväksyttyjen fyysisesti suojattujen alueiden ulkopuolella, aineisto/liikenne salataan viranomaisen ko. suojaustasolle hyväksymällä menetelmällä.	Toteutuu	Aineistoa ei salata, mutta liikenne salataan SSL-tekniikalla.		07.03.2018
2) Kun salassa pidettävää aineistoa siirretään hyväksyttyjen fyysisesti suojattujen alueiden sisäpuolella, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella viranomaisen erillishyväksyntään perustuen.	Ei toteudu	Ei salata.		26.05.2018

Toteutuu: Ei
Muistiinpanot:
Omistaja:
Lisätietoja: I15.pdf
Liitteet:
Luotu: 19.12.2017 Automaattisesti luotu lomake
Päivitetty: 26.05.2018 Lindroos Robin

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.3. Tietoaineistoturvallisuus
Kriteeri: I 16 Aineiston välitys postilla ja kuriirilla
Suojaustaso: IV-II
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
1) Tietojen siirtämisessä yksiköiden ja tilojen välillä fyysisesti suojattujen alueiden ulkopuolella on noudatettava seuraavaa: Yleisenä sääntönä on, että salassa pidettävät tiedot siirretään tietoverkon yli sähköisesti viranomaisen hyväksymillä salaustuotteilla suojattuna.	Toteutuu	Siirretään VPN-tunnelia hyödyntäen.		07.03.2018
2) Tietojen siirtämisessä yksiköiden ja tilojen välillä fyysisesti suojattujen alueiden ulkopuolella on noudatettava seuraavaa: Jos edellä mainittua (vaatimus 1) menettelyä ei käytetä, salassa pidettävät tiedot kuljetetaan joko a) viranomaisen hyväksymillä salaustuotteilla suojatuilla sähköisillä välineillä (kuten USB-muistitikut, CD-levyt, kiintolevyt); tai b) kaikissa muissa tapauksissa, viranomaisen antamia ohjeita noudattaen.	Toteutuu	Pyritään siirtämään vain sähköisiä kanavia pitkin.		07.03.2018

Toteutuu: Kyllä
Muistiinpanot:
Omistaja:
Lisätietoja: I16.pdf
Liitteet:
Luotu: 19.12.2017 Automaattisesti luotu lomake
Päivitetty: 07.03.2018 Lindroos Robin

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.3. Tietoaineistoturvallisuus
Kriteeri: I 17 Tulostus ja kopiointi
Suojaustaso: IV-III
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
1) Jäljennöksiin ja käännöksiin sovelletaan alkuperäistä asiakirjaa koskevia turvatoimia.	Toteutuu	Kopioita käsitellään kuten alkuperäistä asiakirjaa. Kopiolaitteiden käyttö on suojattu ulkopuolisilta.		07.03.2018

Toteutuu: Kyllä
Muistiinpanot:
Omistaja:
Lisätietoja: I17.pdf
Liitteet:
Luotu: 19.12.2017 Automaattisesti luotu lomake
Päivitetty: 07.03.2018 Lindroos Robin

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.3. Tietoaineistoturvallisuus
Kriteeri: I 18 Turvallisuustarkoituksia varten tapahtuva salassa pidettävien tietojen kirjaaminen
Suojaustaso: IV
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
1) Tietojenkäsittely-ympäristössä toteutetaan hallinnolliset ja tekniset toimenpiteet, jotka koskevat salassa pidettävien tietojen valvomista koko niiden elinkaaren ajan, jotta autetaan estämään ja havaitsemaan tällaisten tietojen tahallinen tai tahaton vaarantuminen tai katoaminen.	Toteutuu	Valvotaan ja estetään käyttöoikeuksin. Lokitus päällä. Tiedot varmistetaan varmuuskopioin.		07.03.2018

Toteutuu: Kyllä
Muistiinpanot:
Omistaja:
Lisätietoja: I18.pdf
Liitteet:
Luotu: 19.12.2017 Automaattisesti luotu lomake
Päivitetty: 21.05.2018 Lindroos Robin

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.3. Tietoaineistoturvallisuus
Kriteeri: I 19 Salassa pidettävää tietoa sisältävien tietoaineistojen hävittäminen
Suojaustaso: IV
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
1) Ei-sähköisten aineistojen hävittäminen on järjestetty luotettavasti. Hävittämisessä käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain.	Toteutuu	On ostettu palveluna tuhottavat paperiastiat ja niiden tyhjennykset.		07.03.2018
2) Sähköisten aineistojen hävittäminen on järjestetty luotettavasti. Hävittämisessä käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain.	Toteutuu	Kiintolevyt tuhotaan luotettavasti. USB-muistien käytöstä ja niiden tuhoamisesta ei ole tarkkaa ohjeistusta.		22.05.2018
3) Tietojärjestelmien käytön yhteydessä syntyvät tietoa sisältävät väliaikaistiedostot hävitetään säännöllisesti, jolleivät ne poistu tietojärjestelmästä automaattisesti.	Toteutuu	Tilapäiset tiedostot tyhjenntetään tietoasemilta tarpeen mukaan.		07.03.2018

Toteutuu: Kyllä
Muistiinpanot:
Omistaja:
Lisätietoja: I19.pdf
Liitteet:
Luotu: 19.12.2017 Automaattisesti luotu lomake
Päivitetty: 22.05.2018 Lindroos Robin

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.4. Käyttöturvallisuus
Kriteeri: I 20 Muutoshallintamenettelyt
Suojaustaso: IV-II
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
1) Turvallisuuden varmistamista pidetään vaatimuksena koko tietojenkäsittely-ympäristön elinkaaren ajan sen alullepanosta käytöstä poistamiseen.	Toteutuu	Varmistetaan että laitteiden tietoturva on ajan tasalla koko elinkaaren ajan. Konfiguraatioita tiukennetaan tarpeen mukaan. Elinkaaren eri vaiheissa olevat laitteet on luetteloitu ja tiedossa. (Asset management)		23.03.2018
2) Turvallisuutta koskevat arvioinnit, tarkastukset ja uudelleentarkastelut suoritetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä.	Ei toteudu	Käydään läpi poikkeuksellisten tilanteiden ilmetessä. Muutoksia järjestelmiin pystyvät tekemään nimetyt henkilöt, eikä niitä tämän takia tarkasteta määräajoin.		21.05.2018
3) Tietojenkäsittely-ympäristön turvallisuusasiakirjoja kehitetään sen elinkaaren aikana erottamattomana osana muutosten ja asetusten hallintaprosessia.	Toteutuu	Tietojärjestelmädokumentaatiota päivitetään muutoksia tehdessä.		07.03.2018

Toteutuu: Ei
Muistiinpanot: Muutokset kirjataan tikettijärjestelmään, josta pyynnön tekijä ja muutoksen toteuttaja ovat jäljitettävissä. Muutoksia voi tilata vain yksi henkilö. Muutoksista jää lokiin jälki, joita tarkkaillaan tarvittaessa.
Omistaja:
Lisätietoja: I20.pdf
Liitteet:
Luotu: 19.12.2017 Automaattisesti luotu lomake
Päivitetty: 21.05.2018 Lindroos Robin

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.4. Käyttöturvallisuus
Kriteeri: I 21 Fyysinen turvallisuus
Suojaustaso: IV
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
1) Fyysiset turvatoimet toteutetaan kaikissa tiloissa, rakennuksissa, toimistoissa, huoneissa ja muissa paikoissa, joissa tietoja käsitellään tai säilytetään, tietojenkäsittely-ympäristöjen sijoitusalueet mukaan luettuina.	Ei toteudu	Näytön sivulta katsomisen suojat ovat käytössä. Vierailijat pyritään ottamaan vastaan ja kirjaamaan. Kulku on rajoitettua virka-ajan ulkopuolella ja osassa tiloja koko ajan, mutta fyysiset turvatoimet uupuvat sisäänkäynnin ja toimistotilojen välillä. Ulkoistetun konesalin osalta toimittajlla on asianmukainen sertifiointi (ISO/IEC 27001:2013. Certification number FI150121-1). Omissa tiloissa olevien tietojenkäsittelyn osalta keskeisten tilojen (Konesali, sekä IT tuen huone) on fyysinen lukitus ja avaimet vain rajoitetulla henkilöstöllä.		22.05.2018
2) Tietojen käsittely on mahdollista turva-alueilla, hallinnollisella alueella tai viranomaisen hyväksymillä menettelyillä hallinnollisen alueen ulkopuolella.	Toteutuu	Suojattu VPN-tekniikalla.		07.03.2018
3) Tietojen säilytys on mahdollista turva-alueilla ja hallinnollisella alueella soveltuvissa lukittavissa toimistokalusteissa, tai tilapäisesti myös viranomaisen hyväksymillä menettelyillä hallinnollisen alueen ulkopuolella.	Ei toteudu	Muutoin tietoja säilytetään lukituissa ja valvotuissa tiloissa, mutta käyttäjien työasemien osalta tämä ei mahdollista tilaratkaisujen vuoksi. Työasemien tietoja ei myöskään ole kryptatttu joten mahdollisuus tätä kautta tietuturva-uhkaan olemassa.		23.03.2018

Toteutuu: Ei
Muistiinpanot:

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.4. Käyttöturvallisuus
Kriteeri: I 22 Etäkäyttö ja etähallinta
Suojaustaso: IV
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
1) Tietojen välitys ja käsittely fyysisesti suojattujen alueiden välillä on mahdollista vain viranomaisen ko. suojaustasolle hyväksymien korvaavien menettelyjen mukaisesti.	Ei toteudu	VPN on käytössä, mutta ei perustu multifactor autentikaatioon. VPN salasanaa ei voi tallentaa clienttiin. VPN käyttää Windows AD tunnusta ja salasanaa (Työasema kirjaus tunnukset)		21.05.2018
2) Henkilöstö on koulutettu ja ohjeistettu turvalliseen etäkäyttöön/-hallintaan.	Toteutuu	Etäkäytön mahdollistavan VPN clientin asentamisen yhteydessä henkilöä ohjeistetaan suullisesti VPN käytöstä. Krijallinen ohjeistus uupuu. Työaseman yleisen turvallisen käytön ohjeistus löytyy Intranetista.		23.03.2018
3) Elleivät hyväksyttyjen fyysisesti suojattujen alueiden ulkopuolelle viedyt suojaustason IV tietoa sisältävät tietovälineet (kiintolevyt, USB-muistit ja vastaavat) ole salattu viranomaisen ko. suojaustasolle hyväksymällä menetelmällä, tietovälineet säilytetään vastaavantasoisesti suojaten, kuin hallinnollisen turva-alueen lukittavissa toimistokalusteissa säilytettynä, tai tietovälineitä ei jätetä valvomatta.	Toteutuu	Käyttäjiä on koulutettu arkaluontoisten tietojen käsittelemisessä.		07.03.2018
4) Järjestelmien etäkäyttö-/-hallintaratkaisu edellyttää viranomaisen ko. suojaustasolle hyväksymää liikenteen salausta.	Toteutuu	SSL/VPN suojattu.		07.03.2018

Toteutuu: Ei
Muistiinpanot:
Omistaja:
Lisätietoja: I22.pdf
Liitteet:
Luotu: 19.12.2017 Automaattisesti luotu lomake
Päivitetty: 22.05.2018 Lindroos Robin

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.4. Käyttöturvallisuus
Kriteeri: I 23 Ohjelmistohaavoittuvuuksien hallinta
Suojaustaso: IV-II
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
Tietojenkäsittely-ympäristön koko elinkaaren ajalle toteutetaan luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi.	Toteutuu	Viranomaisten, laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan ja tarpeellisiksi arvioidut turvapäivitykset asennetaan hallitusti. - Seuranta ulkoistettu IT-Kumppanille. Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet ja vastaavat tarkastetaan vähintään (haavoittuvuusskannaus, CMDB, jne.) vuosittain ja aina merkittävien muutosten jälkeen päivitysmenettelyjen korjauskohteiden löytämiseksi. Lisäksi säännöllisesti (esim. kuukausittain) tarkastellaan keskitetyistä päivityksenjakopalveluista päivitysten asentumisen onnistumista. -On keskitetty laitehallinta rekisteri, josta tarkistetaan että laiteet ovat eheät, laitteet ovat verkossa ja päivitykset ovat ajan tasalla sekä poikkeamien sattuessa käydään tarvittaviin toimiin..		07.03.2018

Toteutuu: Kyllä
Muistiinpanot:
Omistaja:
Lisätietoja: I23.pdf
Liitteet:
Luotu: 19.12.2017 Automaattisesti luotu lomake
Päivitetty: 07.03.2018 Lindroos Robin

Osa-alue: 4. Tekninen tietoturvallisuus
Aihe-alue: 4.4. Käyttöturvallisuus
Kriteeri: I 24 Varmuuskopiointi
Suojaustaso: IV-II
Sovelletaan: Sovelletaan
Vaatimukset:

Vaatimus	Tila	Muistiinpanot	Vastuuhenkilö	Päivitetty
Salassa pidettävää tietoa sisältävät varmuuskopiot suojataan niiden elinkaaren ajan vähintään vastaavan tasoisilla menetelmillä, kuin millä alkuperäinen tieto.	Toteutuu	1. Varmistusten taajuus on riittävä varmistettavan tiedon kriittisyyteen nähden. Edellyttää selvitystä siitä, kuinka paljon dataa voidaan menettää - Taajuus on riittävä (recovery point objective, RPO). 2. Palautusprosessin nopeus on riittävä toimintavaatimuksiin nähden. Edellyttää selvitystä siitä, kuinka kauan palautuminen voi kestää (recovery time objective, RTO). - Riittävän nopea ja tarkistetaan tarvittaessa. 3. Varmuuskopioinnin ja palautusprosessin oikea toiminta testataan säännöllisesti. - Toimimattomasta varmuuskopiosta tulee häkytys IT-toimittajalle ja palautusta testataan sovituksen mukaisesti. 4. Palautusprosessin dokumentointi on riittävällä tasolla. -On dokumentoitu ja opastettu IT-henkilöstölle. 5. Varmuuskopioiden fyysinen sijoituspaikka on riittävän eriytetty varsinaisesta järjestelmästä (eri sortuma-/palotila, välimatka varmuuskopion ja varsinaisen tilan välillä, jne.). Huom: Varmuuskopiot tulisi suojata fyysisen ja loogisen pääsynhallinnan menetelmin vähintään tiedon (mahdollisesti kasautumisvaikutuksen nostaman) suojaustason mukaisesti. - Säilytetään eri rakennuksessa. 6. Käsiteltäessä samalla varmistusjärjestelmällä eri omistajien tietoja, tarkastusoikeuden (vrt. I 06) mahdollistavat erottelumenettelyt on toteutettava varmistusjärjestelmän liittymien ja tallennemedioiden osalta (esim. omistaja-/hankekohtaiset eri avaimilla salatut nauhat, joita säilytetään asiakaskohtaisissa kassakaapeissa/ kassakaappilokeroissa). - Käsitellään samalla materiaalilla, mutta erotusmenettelyjä ei ole.		07.03.2018

Toteutuu: Kyllä
Muistiinpanot:
Omistaja:
Lisätietoja: I24.pdf
Liitteet:
Luotu: 19.12.2017 Automaattisesti luotu lomake